VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Energetické spektrum částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky z hlediska teorie čísel

Energetic spectrum of a particle in three-dimensional infinite potential square well in terms of number theory

2016 David Ulčák

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Zadání bakalářské práce

Student: **David Ulčák**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 1103R031 Výpočetní matematika

Téma: Energetické spektrum částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky z hlediska teorie čísel
Energetic spectrum of a particle in three-dimensional infinite potential square well in terms of number theory

Jazyk vypracování: čeština

Zásady pro vypracování:

V kvantové fyzice zavádíme model částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky. Řešením stacionární Schrödingerovy rovnice obdržíme spektrum povolených energií této částice. Pokud zvolíme vhodné jednotky energie (pro konkrétní potenciálovou jámu), pak toto spektrum povolených energií představuje z hlediska teorie čísel zajímavou množinu přirozených čísel vyjádřitelných ve tvaru součtu druhých mocnin přirozených čísel.Bakalářská práce by měla obsahovat:

1. Stručný úvod do teorie kvantové mechaniky použité při řešení modelu částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky.

2. Podrobné řešení modelu částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky.
3. Uvedení zjištěného spektra povolených energií do souvislosti s poznatky teorie čísel (tj. popis známých vlastností množiny přirozených čísel ve tvaru součtu tří druhých mocnin přirozených čísel).

Seznam doporučené odborné literatury:

[1] Kolibiar M., Legéň A., Šalát T., Znám Š.: Algebra a príbuzné disciplíny, Bratislava, Alfa, 1992.
[2] Beiser A.: Perspectives of Modern Physics, New York, McGraw-Hill, 1969.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **RNDr. Pavel Jahoda, Ph.D.**

Datum zadání: 01.09.2015

Datum odevzdání: 29.04.2016

doc. RNDr. Jiří Bouchala, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 29. dubna 2016 .....

Rád bych na tomto místě poděkoval panu RNDr. Pavlu Jahodovi, Ph.D. za přínosné konzultace, rady a trpělivé vedení práce, dále panu Ing. Janu Kracíkovi, Ph.D. za konstrukci a vysvětlení Bayesovského odhadu v Kapitole 5, a paní Mgr. Janě Trojkové, Ph.D. za pomoc s pochopením základů kvantové mechaniky pro Kapitolu 2.

Abstrakt

V této bakalářské práci se budeme zabývat myšlenkovým modelem částice uzavřené v nepropustnutelné nádobě, již zveme potenciálová jáma. Text začíná stručným úvodem k tématu, následovaným některými základními pojmy a úvodem do problematiky kvantové mechaniky, při němž se seznámíme se Schrödingerovou rovnicí, kterou pak pro výše zmíněný model vyřešíme. Obdržíme tak diskrétní spektrum energií částice, jež je při vhodné volbě jednotek ekvivalentní s množinou čísel, vyjádřitelných jako součet tří druhých mocnin přirozených čísel. Na množinu těchto čísel se podíváme podrobněji, seznámíme se s problematikou součtu čtverců celých čísel a asymptotickou hustotou. V závěru práce zkonstruujeme myšlenkový experiment s měřením energií a pokusíme se na základě získaných výsledků zjistit počet částic v jámě pomocí statistických metod.

Klíčová slova: kvantová fyzika, Schrödingerova rovnice, teorie čísel, součet druhých mocnin celých čísel, asymptotická hustota, testování statistických hypotéz, Bayesovské metody

Abstract

In this bachelor thesis we will be concerned with mental model of a particle enclosed within impenetrable container, which we call potential well. The text begins with brief introduction to the topic, followed by some basic concepts and the introduction to quantum mechanics, during which we will get acquainted with Schrödinger equation, which will be solved then for above mentioned model. This way, we will recieve discrete spectrum of energies of a particle, which is, by suitable choice of units, equivalent to set of numbers, expressible as a sum of three squares of natural numbers. We will take a close look at this set and get acquainted with issues of sums of integer squares and asymptotic density. In the end of the thesis, we will construct mental experiment with energy measuring and, on the basis of the acquired results, we will try to find out the count of particles in the well using statistical methods.

Key Words: quantum physics, Schrödinger equation, number theory, sum of squares of integers, asymptotic density, statistical hypothesis testing, Bayesian methods

Obsah

Seznam použitých zkratek a symbolů

$\cup$	–	sjednocení
$\cap$	–	průnik
$\overline{A}$	–	doplněk k množině/jevu A
$\propto$	–	přímá úměra
Δ	–	Laplaceův operátor, $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$
$\gcd(a, b)$	–	největší společný dělitel čísel a, b
h	–	Planckova konstanta, $h = 6,626 \cdot 10^{-34}$ J·s
$\hbar$	–	redukovaná Planckova konstanta, $\hbar = \frac{h}{2\pi}$
m	–	hmotnost, kg
p	–	hybnost, kg·m·s^{-1}
V	–	potenciální energie, J
v	–	rychlost, m·s^{-1}
$\mathbb{N}$	–	množina přirozených čísel
$\mathbb{R}$	–	množina reálných čísel
$\mathbb{R}^+$	–	množina kladných reálných čísel
$\mathbb{Z}$	–	množina celých čísel
$\mathbb{Z}_0^+$	–	množina nezáporných celých čísel

Seznam obrázků

Seznam tabulek

Seznam výpisů zdrojového kódu

1 Úvod

Jak již můžeme vědět z jiných odvětví, pod pojmem spektrum máme na mysli určitou škálu nabývaných hodnot jisté veličiny. Není tedy překvapením, že energetické spektrum částice představuje jakousi množinu, sestávající z energetických hladin, jichž může částice nabývat.

Abychom se však mohli zabývat tak malými objekty, jako jsou částice, nevystačíme s klasickou fyzikou. Ta byla v mikrosvětě před necelým stoletím nahrazena fyzikou kvantovou a její výsledky úspěšně ukazují na to, že se nejednalo jen o nahodilou konstrukci, nýbrž o velký průlom v oblasti fyziky. Jako jedna ze základních ukázek aplikací kvantové mechaniky v praxi se užívá model potenciálové jámy. Tento model lze za určitých podmínek použít jako aproximaci reálné situace pohybu elektronu, a především je na něm možno pochopit nejzákladnější principy tohoto stále se vyvíjejícího odvětví.

Při řešení problému částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky se pak ukáže, že je energie spjata se součtem tří druhých mocnin přirozených čísel. A tu nás napadne se na množinu těchto čísel podívat z matematického hlediska. Problémem součtu druhých mocnin celých čísel se v historii zabývali Pierre de Fermat, Joseph-Louise Lagrange, Adrien-Marie Legendre, Leonhard Euler, Carl Friedrich Gauss a další jména slavná nejen v teorii čísel, ale v celé matematice a vědě obecně. Některé z jejich poznatků použijeme ke zkoumání energetického spektra částice i v této práci.

Jelikož rovina, v níž se budeme pohybovat bude velmi teoretická, dává nám to možnost lehce popustit uzdu fantazii a v rámci energií si sestavit myšlenkový experiment, jehož idea byla stručně nastíněna již v [6], a na kterém budeme prezentovat některé statistické metody. Tímto provázáním tří pouze zdánlivě nesourodých vědeckých disciplín dostala tato práce svou finální podobu. Kéž čtenáři přinese zábavu i ponaučení.

2 Energetické spektrum částice

V první části této kapitoly uvedeme základní pojmy, především z oblasti statistiky, a seznámíme se se základními vztahy v kvantové mechanice, problémem částice v nekonečné potenciálové jámě a jeho řešením.

2.1 Základní pojmy

Na začátku se dohodněme, že **náhodným pokusem** nazveme každý konečný děj, jehož výsledek nelze předem s jistotou stanovit. Množinu Ω, obsahující všechny možné (navzájem se vylučující) výsledky náhodného pokusu označujme jako **prostor elementárních jevů**.

Definice 2.1 *Nechť Ω je libovolná množina a $S \subseteq 2^{\Omega}$. Množinu S potom nazveme **σ-algebrou**, pokud platí:*

1. $\emptyset \in S$
2. $A \in S \quad \Rightarrow \quad \overline{A} = \Omega - A \in S$
3. $A_1, A_2, A_3, \ldots \in S \quad \Rightarrow \quad \bigcup_{i=1}^{\infty} A_i \in S.$

Definice 2.2 *Nechť Ω tvoří prostor elementárních jevů a $S \subseteq 2^{\Omega}$ je nějaká jemu příslušející σ-algebra. Dále nechť P je takové zobrazení $S \to \langle 0, 1 \rangle$, splňující*

1. $P(\emptyset) = 0$
2. $P(\overline{A}) = 1 - P(A)$
3. $A_1, A_2, A_3, \ldots \in S,\ A_i \cap A_j = \emptyset \quad \Rightarrow \quad P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i).$

*Pak uspořádanou trojici (Ω, S, P) nazveme **pravděpodobnostním prostorem**.*

Množině S říkáme prostor jevů, zobrazení P označujeme jako pravděpodobnostní míru.

Definice 2.3 *Nechť (Ω, S, P) je pravděpodobnostní prostor. **Náhodnou veličinou** nazveme zobrazení $X : \Omega \to \mathbb{R}$ právě tehdy, když pro každé $x \in \mathbb{R}$ platí*

$$\{\omega | \omega \in \Omega,\ X(\omega) < x\} \in S \quad \vee \quad \{\omega | \omega \in \Omega,\ X(\omega) > x\} \in S.$$

*Náhodnou veličinu X dále nazveme **diskrétní**, jestliže nabývá pouze konečně, či spočetně mnoha hodnot, v opačném případě hovoříme o **spojité** náhodné veličině.*

Náhodná veličina tedy vyjadřuje jakousi numerickou míru či hodnotu náhodných jevů. Označení $P(X = x)$ (respektive $P(X > x)$, případně $P(X < x)$) pak znamená pravděpodobnost, že náhodná veličina X nabývá hodnoty (případně je větší/menší, než) x.

Definice 2.4 ***Distribuční funkcí*** *náhodné veličiny X nazveme funkci $F : \mathbb{R} \to \langle 0, 1\rangle$ takovou, že*

$$\forall t \in \mathbb{R} : F(t) = P(X < t).$$

Pro diskrétní náhodnou veličinu dále definujeme ***Pravděpodobnostní funkci*** *jako*

$$P(x) = P(X = x),$$

pro spojitou náhodnou veličinu zase zavádíme ***hustotu pravděpodobnosti*** *vztahem*

$$f(t) = F'(t).$$

Při zápise většinou, pokud to není nevyhnutelně nutné, nerozlišujeme náhodnou veličinu a její hodnotu. Poznamenejme ještě, že mezi distribuční a pravděpodobnostní funkcí (pro diskrétní náhodnou veličinu), resp. distribuční funkcí a hustotou pravděpodobnosti, platí tyto vztahy:

$$F(x) = \sum_{x_i<x} P(X = x_i), \text{ resp. } F(x) = \int_{-\infty}^{x} f(t)\mathrm{d}t.$$

Pod pojmem **rozdělení pravděpodobnosti** náhodné veličiny X pak rozumíme konkrétní předpis pro její distribuční, či pravděpodobnostní funkci, popř. pro hustotu pravděpodobnosti. O základních charakteristikách většiny nejpoužívanějších jak diskrétních, tak spojitých rozdělení náhodné veličiny se lze dočíst například v [5].

Poznámka 2.1 Uspořádanou n-tici náhodných veličin nazýváme **náhodný vektor**, v souvislosti s jeho spojitou variantou se pak hovoří o **sdružené hustotě pravděpodobnosti** $f(x_1, x_2, \ldots, x_n)$, a dále o sdružené distribuční funkci $F(x_1, x_2, \ldots, x_n)$, přičemž platí

$$F(x_1, x_2, \ldots, x_n) = \int \cdots \int f(x_1, x_2, \ldots, x_n)\mathrm{d}x_1\mathrm{d}x_2 \ldots \mathrm{d}x_n.$$

Důvod proč zde zavádíme pojmy z oblasti statistiky je prostý - jednak se statistikou budeme zabývat v Kapitole 5, a především, pravděpodobnostní přístup je jednou ze základních myšlenek kvantové mechaniky, jak záhy uvidíme.

Definice 2.5 ***Vlnovou rovnicí*** *nazveme každou lineární homogenní parciální diferenciální rovnici ve tvaru*

$$\Delta\psi(\mathbf{r}, t) - \frac{1}{c^2}\frac{\partial^2\psi}{\partial t^2}(\mathbf{r}, t) = 0, \tag{2.1}$$

její řešení pak nazýváme ***vlnovou funkcí****.*

Dodejme, že konstanta c je parametr rychlosti šíření vlny. Tato diferenciální rovnice popisuje obecně takřka jakýkoliv typ vlnění, pro odvození viz [9].

2.2 Postuláty kvantové mechaniky a vlnová funkce Ψ

Tak jako se matematika opírá o axiomy, kvantová mechanika má své postuláty, tedy fundamentální výroky, které jsou vesměs považovány za dostatečně experimentálně ověřené, ergo platné. Abychom byli trochu lépe tuto fyzikální oblast schopni pojmout, postuláty zde uvedeme (viz [2]).

Postulát 1 (O vlnové funkci Ψ) *Veškeré informace o kvantovém stavu částice jsou obsaženy ve vlnové funkci ψ, tedy komplexní funkci o 4 proměnných - 3 prostorových a jedné časové. Dále předpokládáme, že hustota pravděpodobnosti výskytu částice v prostoru V, v místě $\mathbf{r}$ (hovoříme o polohovém vektoru $\mathbf{r}$) a čase t je rovna kvadrátu absolutní hodnoty ψ.*

Odtud můžeme na ψ klást normovací podmínku pro integraci přes celý prostor V:

$$\int |\psi(\mathbf{r},t)|^2 \mathrm{d}V = 1.$$

S tímto pravděpodobnostním přístupem vyvstávají následující požadavky na funkci ψ, která tedy musí být

1. spojitá,
2. konečná,
3. jednoznačná (ve smyslu komplexní funkce),
4. integrovatelná s kvadrátem a
5. při konečných změnách potenciálu musí mít spojité parciální derivace $\frac{\partial\psi}{\partial x}, \frac{\partial\psi}{\partial y}, \frac{\partial\psi}{\partial z}$.

Postulát 2 (O operátorech) *Každé měřitelné fyzikální veličině je přiřazen operátor (lineární a hermitovský), působící na vlnovou funkci.*

Postulát 3 (O kvantování) *Při jednotlivých měřeních veličiny X můžeme naměřit pouze a jedině vlastní hodnoty x_n příslušného operátoru $\widehat{X}$, tedy takové hodnoty x_n, pro něž platí*

$$\widehat{X}\psi_n = x_n\psi_n.$$

V případě, že je v okamžiku měření systém popsán vlnovou funkcí ψ, je střední hodnota opakovaných měření veličiny X daná vztahem

$$\overline{X} = \left(\psi, \widehat{X}\psi\right) = \int \psi^*(\mathbf{r},t)\widehat{X}\psi(\mathbf{r},t)\mathrm{d}V,$$

kde ψ^* označuje funkci komplexně sdruženou s ψ.

Poslední dva z výše uvedených postulátů úzce souvisí s funkcionální analýzou. Pokud se totiž na ψ díváme jako na prvek nekonečnědimenzionálního Hilbertova prostoru (pro bližší seznámení viz například [10]), pak z jejích souřadnic vzhledem k příslušné ortonormální bázi můžeme přímo určit pravděpodobnost, že naměříme konkrétní hodnotu x_n měřené veličiny X, čehož se v kvantové mechanice velmi často využívá.

Postulát 4 (O redukci vlnové funkce) *Naměřením konkrétní hodnoty x_n veličiny X převedeme systém do stavu s vlnovou funkcí ψ_n, která je vlastní funkcí operátoru $\widehat{X}$, a příslušející jeho vlastnímu číslu x_n.*

Jinými slovy, měření samotné ovlivňuje kvantový stav systému a tedy i mění jeho vlnovou funkci.

Postulát 5 (O časové Schrödingerově rovnici) *Jestliže v čase t_0 je systém popsaný vlnovou funkcí $\psi(\mathbf{r}, t_0)$, jeho další vývoj je popsán časovou Schrödingerovou rovnicí*

$$i\hbar\frac{\partial\psi}{\partial t} = \widehat{H}\psi,$$

kde operátor $\widehat{H}$ se nazývá Hamiltonián a jedná se o operátor celkové energie systému.

Poznámka 2.2 V dalších úvahách budeme užívat variantu Hamiltoniánu pro volnou částici ve tvaru $\widehat{H} = -\frac{\hbar^2}{2m}\Delta + V$.

Schrödingerova rovnice je svým způsobem variantou vlnové rovnice pro popis vlnových vlastností částic, funkce ψ pak jejím řešením pro daný stav.

Původně se mělo za to, že vlnově lze nahlížet pouze na nehmotné částice. S myšlenkou, že určité vlnové vlastnosti vykazují i hmotné částice přišel v roce 1924 francouzský fyzik Louis de Broglie, po němž bylo také ono vlnění pojmenováno. Toto vlnění je pro volnou částici charakterizováno **de Broglieho vlnovou délkou**

$$\lambda = \frac{h}{p}, \tag{2.2}$$

kde h je Planckova konstanta a p je hybnost částice.

2.3 Stacionární Schrödingerova rovnice

Při uvádění postulátů v minulém pododdíle asi nejvíc otázek vzbuzuje ten poslední, o časové Schrödingerově rovnici. Nabízí se totiž přirozená otázka, proč tato rovnice vypadá zrovna tak, jak vypadá. Velice zjednodušenou ilustraci jejího původu nám může dát srovnání s obecnou vlnovou rovnicí.

Uvažujme řešení vlnové rovnice pro rovinnou vlnu ve tvaru

$$\begin{aligned} \psi(\mathbf{r}, t) &= e^{i(\mathbf{kr}-\omega t)}, \\ \text{kde } \mathbf{k} &= \frac{2\pi}{\lambda} = \frac{p}{\hbar}, \end{aligned} \tag{2.3}$$

přičemž $\mathbf{k}$ nazýváme vlnový vektor a $\hbar$ je redukovaná Planckova konstanta. Dosazením do vlnové rovnice (2.1) vzniká

$$\left(-k^2 + \frac{\omega^2}{c^2}\right)\psi = 0,$$

odtud vyplývá $\omega = kc$. Pokud tedy Laplaceův operátor neaplikujeme a pouze pro druhého sčítance v rovnici (2.1) užijeme právě nalezeného vztahu pro ω a vztahu (2.3), získáme

$$\begin{aligned} \left(\Delta + k^2\right)\psi &= 0 \\ \left(\Delta + \tfrac{p^2}{\hbar^2}\right)\psi &= 0. \end{aligned} \tag{2.4}$$

Nyní uvažme zákonitosti klasické mechaniky. Celková mechanická energie objektu je dána vztahem $E = T + V$, kde T označuje kinetickou a V potenciální energii. Pro hybnost a kinetickou energii v Newtonovské mechanice pak platí

$$\begin{aligned} p &= mv \\ T &= \tfrac{1}{2}mv^2 = \tfrac{p^2}{2m}, \end{aligned}$$

a tak můžeme p^2 vyjádřit jako

$$p^2 = 2m(E - V). \tag{2.5}$$

Dosazením vztahu (2.5) do (2.4) získáme

$$\underbrace{\left(-\frac{\hbar^2}{2m}\Delta + V\right)}_{=\ \widehat{H}\ \text{pro volnou částici}}\psi = E\psi. \tag{2.6}$$

Zbývalo by ukázat, že $E\psi = i\hbar\frac{\partial\psi}{\partial t}$. To posléze z předpokladu platnosti Schrödingerovy rovnice uvidíme při zavedení její stacionární varianty, kterou se budeme zabývat dále.

Poznámka 2.3 Nutno zdůraznit, že se nejedná o korektní odvození, ale pouhou ilustraci, a tvar časové Schrödingerovy rovnice je jakožto postulát brán jako holý fakt. Kvůli odlišnostem klasické a kvantové mechaniky totiž nelze přímo matematicky odvodit příslušný aparát.

Stacionární Schrödingerovu rovnici uvažujeme pro případy, kdy se nebere v potaz závislost

působících sil na čase. Z tohoto důvodu lze uvážit zápis vlnové funkce ve tvaru

$$\psi(\mathbf{r}, t) = \psi(\mathbf{r})\varphi(t).$$

Dosazením do časové Schrödingerovy rovnice pak dostáváme:

$$\begin{aligned} i\hbar\left(\varphi(t)\cdot\frac{\mathrm{d}\psi(\mathbf{r})}{\mathrm{d}t}+\psi(\mathbf{r})\cdot\frac{\mathrm{d}\varphi(t)}{\mathrm{d}t}\right) &= \widehat{H}\psi(\mathbf{r})\varphi(t) \\ \frac{i\hbar}{\varphi(t)}\frac{\mathrm{d}\varphi(t)}{\mathrm{d}t} &= \frac{\widehat{H}\psi(\mathbf{r})}{\psi(\mathbf{r})}. \end{aligned} \tag{2.7}$$

Poněvadž rovnost (2.7) musí platit v libovolném čase t a místě $\mathbf{r}$, pak musí být obě strany rovny konstantě, označme ji E. Přepíšeme-li nyní obě strany rovnosti (2.7) zvlášť, dostáváme

$$i\hbar\frac{\mathrm{d}\varphi(t)}{\mathrm{d}t} = E\varphi(t) \tag{2.8}$$

$$\widehat{H}\psi(\mathbf{r}) = E\psi(\mathbf{r}), \tag{2.9}$$

přičemž vztah (2.9) označujeme jako **stacionární Schrödingerovu rovnici**, zatímco (2.8) dokresluje hrubý nástin Schrödingerovy rovnice uvedený dříve. Pro další výpočty si ještě stacionární Schrödingerovu rovnici zapíšeme v následujícím tvaru:

$$\Delta\psi + \frac{2m}{\hbar^2}(E - V)\psi = 0. \tag{2.10}$$

Poznámka 2.4 Jak ze zápisu (2.9) vidíme, konstanta E je vlastním číslem Hamiltoniánu, s ohledem na Postulát 3 se tedy jedná o hodnotu energie pro daný stav.

2.4 Částice v trojrozměrné potenciálové jámě

Jde o myšlenkový model částice v ohraničené oblasti. Rozumíme tím pomyslnou oblast, v níž je všude $V = 0$, čili veškerá energie částice je dána její energií kinetickou. Jámu si lze zjednodušeně představit jako jakousi nádobu, která omezuje pohyb částice. Jak říká název této práce, my se budeme zabývat jednoduchou variantou, **trojrozměrnou pravoúhlou potenciálovou jámou nekonečné hloubky**. Nekonečná hloubka potenciálové jámy se dá interpretovat tak, že stěny oné pomyslné nádoby mají nekonečnou tuhost, takže částice při srážkách se stěnou neztrácí nic ze své energie, zároveň má částice uvažovanou potenciální energii mimo nádobu $V = \infty$, čili je nemožné, aby částice z nádoby unikla. Samozřejmě lze uvažovat i jámy, jejichž hloubka není nekonečná, tj. brát v potaz tuhost stěn i polohovou energii částice vně nádoby jako konečná čísla. Stejně tak lze říct, že obecně může jáma nabývat libovolného tvaru (například *toroidu* s ohledem na tvar magnetického pole) a ne pouze pravoúhlého útvaru, jako v našem případě.

Představme si tedy částici uzavřenou v krychli o hraně délky l. Vzhledem k definici jámy víme, že $\psi = 0$ pro $x \notin (0;l) \vee y \notin (0;l) \vee z \notin (0;l)$. Hledáme tedy ψ splňující stacionární Schrödingerovu rovnici a s ohledem na požadavek spojitosti ψ, tedy také okrajovou podmínku $\psi = 0$ na stěnách krychle. Jelikož v prostoru je ψ funkce tří proměnných, musíme tyto proměnné separovat, abychom našli řešení. Pro zjednodušení proto uvažujeme, že pro každou souřadnici existuje vlastní vlnová funkce a celková je pak jednoduše dána součinem dílčích, tedy

$$\psi(x,y,z) = \psi_x(x)\psi_y(y)\psi_z(z).$$

Dosazením do (2.10) a patřičnou úpravou vzniká

$$\frac{1}{\psi_x}\frac{\mathrm{d}^2\psi_x}{\mathrm{d}x^2} + \frac{1}{\psi_y}\frac{\mathrm{d}^2\psi_y}{\mathrm{d}y^2} + \frac{1}{\psi_z}\frac{\mathrm{d}^2\psi_z}{\mathrm{d}z^2} = -\frac{2mE}{\hbar^2}. \tag{2.11}$$

Všimněme si, že sčítance na levé straně jsou již funkcemi jen jedné proměnné. Vidíme, že každý člen na levé straně závisí pouze na jedné souřadnici, zatímco na pravé straně je konstanta (energie pro daný stav). Jinými slovy můžeme uvažovat, že každý člen na levé straně se rovná nějaké dílčí konstantě:

$$\frac{1}{\psi_x}\frac{\mathrm{d}^2\psi_x}{\mathrm{d}x^2} = -k_x^2 \tag{2.12}$$

$$\frac{1}{\psi_y}\frac{\mathrm{d}^2\psi_y}{\mathrm{d}y^2} = -k_y^2 \tag{2.13}$$

$$\frac{1}{\psi_z}\frac{\mathrm{d}^2\psi_z}{\mathrm{d}z^2} = -k_z^2 \tag{2.14}$$

$$k_x^2 + k_y^2 + k_z^2 = \frac{2mE}{\hbar^2}. \tag{2.15}$$

Proč jsme brali v potaz konstanty ve formě druhých mocnin bude záhy patrné. Jak vidíme, všechna tři řešení budou vzájemně analogická, vyřešme například rovnici pro ψ_x.

Tím, že uvažujeme funkce jedné proměnné, řešíme obyčejné diferenciální rovnice. Přepišme si tedy dílčí rovnici (2.12) do následujícího tvaru:

$$\psi_x^{''} + k_x^2\psi_x = 0. \tag{2.16}$$

Jak vidíme, jedná se o homogenní lineární diferenciální rovnici druhého řádu s konstantními koeficienty. Připomeňme, že lineární diferenciální rovnicí druhého řádu se rozumí diferenciální rovnice ve tvaru $y^{''} + a(x)y^{'} + b(x)y = c(x)$. Tuto pak nazýváme homogenní, jestliže $c(x) = 0$ a v případě, že funkce $a(x), b(x)$ jsou konstantní, říkáme, že rovnice je s konstantními koeficienty.[1]

Řešení takovýchto rovnic obecně vede na $y(x) = \mathrm{e}^{\lambda x}$. Dosazením do rovnice (2.16) pak

[1] Pro podrobnější výklad o definici, vlastnostech a řešení obyčejných diferenciálních rovnic viz [8].

získáváme

$$\lambda^2 \mathrm{e}^{\lambda x} + k_x^2 \mathrm{e}^{\lambda x} = 0.$$

Jelikož člen $\mathrm{e}^{\lambda x}$ nikdy nemůže být nulový, můžeme jím celou rovnici podělit, čímž vzniká tzv. charakteristický polynom, jehož kořeny jsou určující pro fundamentální systém řešení naší rovnice:

$$\begin{aligned} \lambda^2 + k_x^2 &= 0 \\ \lambda &= \pm k_x i \\ \varphi_1(x) = \mathrm{e}^{k_x i x},\ \varphi_2(x) &= \mathrm{e}^{-k_x i x}. \end{aligned} \tag{2.17}$$

Obecné řešení je libovolnou lineární kombinací funkcí fundamentálního systému, takže víme, že hledaná funkce ψ_x bude obecně vypadat následovně:

$$\begin{aligned} \psi_x &= C_1 \mathrm{e}^{k_x i x} + C_2 \mathrm{e}^{-k_x i x} = \\ &= C_1 \Big(\cos(k_x x) + i \sin(k_x x) \Big) + C_2 \Big(\cos(-k_x x) + i \sin(-k_x x) \Big) = \\ &= (C_1 + C_2) \cos(k_x x) + i (C_1 - C_2) \sin(k_x x), \qquad C_1, C_2 \in \mathbb{R}. \end{aligned}$$

Ke konkrétnějšímu řešení potřebujeme okrajové podmínky, které jsou v našem případě dány potenciálovou jámou. Víme tedy, že

$$\begin{aligned} \psi_x(0) &= 0 \\ \psi_x(l) &= 0. \end{aligned}$$

Nejprve dosadíme první okrajovou podmínku. Odtud

$$\begin{aligned} (C_1 + C_2) \cos 0 + i(C1 - C2) \sin 0 = 0 \\ C_2 = -C_1. \end{aligned}$$

Následným dosazením druhé okrajové podmínky a zjištěného vztahu mezi konstantami C_1 a C_2 získáváme

$$\begin{aligned} (C_1 - C_1) \cos(k_x l) + i(C_1 + C_1) \sin(k_x l) = 0 \\ 2 C_1 i \sin(k_x l) = 0 \\ \sin(k_x l) = 0 \qquad \Rightarrow \qquad k_x = \frac{a\pi}{l},\ a \in \mathbb{Z}. \end{aligned} \tag{2.18}$$

A konečně, položíme-li $2C_1 i = B$, vzniká nám výsledná dílčí vlnová funkce ψ_x ve tvaru

$$\psi_x = B \sin \frac{a\pi x}{l}, \qquad a \in \mathbb{Z}. \tag{2.19}$$

Zbylé 2 dílčí rovnice pro ψ_y i ψ_z, včetně podmínek pro konstantu k_y, respektive k_z, bychom řešili analogicky a tak můžeme psát celkovou vlnovou funkci ve tvaru

$$\psi(x,y,z) = N \sin \frac{a\pi x}{l} \sin \frac{b\pi y}{l} \sin \frac{c\pi z}{l} \tag{2.20}$$
$$a, b, c \in \mathbb{N}.$$

Poznámka 2.5 Ačkoliv při předchozím průběhu řešení Schrödingerovy rovnice jsme číslo a i čísla b, c (s ohledem na analogii dílčích řešení) označili za celá, kvůli samotné vlnové funkci jsme tento závěr museli poněkud poupravit. Ve vztahu (2.20) jsme tak čísla a, b, c označili za přirozená, neboť v případě, že by kterékoliv z těchto čísel bylo rovno 0, částice by neexistovala (vlnová funkce a tedy i hustota pravděpodobnosti by měly ve všech místech potenciálové jámy nulovou hodnotu). Navíc obecně platí $a^2 = (-a)^2$, resp. $\sin \frac{a\pi}{l} = -\sin\left(-\frac{a\pi}{l}\right)$, přičemž znaménko před funkcí sin lze zahrnout do normovací konstanty N, proto nemá smysl uvažovat čísla a, b, c jako záporná.

Posledním krokem je určení příslušné normovací konstanty N. Z požadavku

$$\int\limits_{\mathbb{R}^3} |\Psi|^2 \mathrm{d}V = 1$$

dostáváme[2]

$$\iiint\limits_{\langle 0,l\rangle^3} |N|^2 \sin^2 \frac{a\pi x}{l} \sin^2 \frac{b\pi y}{l} \sin^2 \frac{c\pi z}{l} \mathrm{d}x\mathrm{d}y\mathrm{d}z = 1$$

$$|N|^2 \cdot \left(\int_0^l \frac{1 - \cos\frac{2a\pi x}{l}}{2} \mathrm{d}x \right) \cdot \left(\int_0^l \frac{1 - \cos\frac{2b\pi y}{l}}{2} \mathrm{d}y \right) \cdot \left(\int_0^l \frac{1 - \cos\frac{2c\pi z}{l}}{2} \mathrm{d}z \right) = 1$$

$$|N|^2 \cdot \left(l - \int_0^l \cos \frac{2a\pi x}{l} \mathrm{d}x \right) \cdot \left(l - \int_0^l \cos \frac{2b\pi y}{l} \mathrm{d}y \right) \cdot \left(l - \int_0^l \cos \frac{2c\pi z}{l} \mathrm{d}z \right) = 8$$

$$|N|^2 \cdot \left(l - \frac{l}{2a\pi} \left[\sin \frac{2a\pi x}{l} \right]_0^l \right) \cdot \left(l - \frac{l}{2b\pi} \left[\sin \frac{2b\pi y}{l} \right]_0^l \right) \cdot \left(l - \frac{l}{2c\pi} \left[\sin \frac{2c\pi z}{l} \right]_0^l \right) = 8$$

[2] $\cos x = \cos^2 \frac{x}{2} - \sin^2 \frac{x}{2} = 1 - 2\sin^2 \frac{x}{2} \quad \Rightarrow \quad \sin^2 \frac{x}{2} = \frac{1-\cos x}{2}$

$$|N|^2 \cdot l^3 = 8$$
$$N = \sqrt{\frac{8}{l^3}}.$$

Výsledná vlnová funkce má tedy předpis

$$\psi(x,y,z) = \sqrt{\frac{8}{l^3}} \sin\frac{a\pi x}{l} \sin\frac{b\pi y}{l} \sin\frac{c\pi z}{l} \tag{2.21}$$
$$a, b, c \in \mathbb{N}.$$

S ohledem na (2.15) se dostáváme ke kýženému energetickému spektru částice. Je patrné, že energie může nabývat jen konkrétních hodnot, aby ψ byla skutečně řešením Schrödingerovy rovnice. Dosazením za konstanty k_x, k_y a k_z do (2.15) a úpravou dostáváme:

$$\frac{a^2\pi^2}{l^2} + \frac{b^2\pi^2}{l^2} + \frac{c^2\pi^2}{l^2} = \frac{2mE}{\hbar^2}$$
$$E = (a^2 + b^2 + c^2)\frac{\hbar^2\pi^2}{2ml^2} \tag{2.22}$$
$$a, b, c \in \mathbb{N}.$$

Čísla a, b, c popisují stav částice a nazýváme je **kvantová čísla**. Závěrem poznamenejme, že jedné konkrétní hodnotě energie může odpovídat více stavů. Například může dojít k různému uspořádání stejných hodnot mezi kvantovými čísly, případně mohou dvě různé trojice druhých mocnin dávat totéž číslo. Takovéto energetické hladiny se označují jako **degenerované**. Jedné degenerované hladině energie tedy odpovídá více kvantových stavů, které si sice odpovídají hodnotou energie částice, ale hodnotami jiných veličin se vzájemně liší. Například kvantové stavy, odpovídající $a = 3,\ b = 2,\ c = 1$ a $a = 1,\ b = 3,\ c = 2$ jsou různé, ale přísluší jim stejná energetická hladina, totéž lze říct o stavech $a = 5,\ b = 1,\ c = 1$ a $a = 3,\ b = 3,\ c = 3$. V Kapitole 4 si mimo jiné ukážeme, že takovýchto stavů je převážná většina.

3 Tvar spektra v kontextu teorie čísel

Jak jsme viděli, energie částice závisí na jejím kvantovém stavu, jenž je charakterizován jako součet tří druhých mocnin přirozených čísel. Zamysleme se, jaká čísla se takto dají vyjádřit. Poznatky této kapitoly byly s menšími úpravami převzaty z [4].

3.1 Přirozená čísla ve tvaru součtu dvou druhých mocnin celých čísel

Věty o vyjádřitelnosti přirozených čísel ve tvaru součtu čtverců se vážou ke čtvercům celých čísel, máme tedy situaci zkomplikovanou požadavkem na nenulová kvantová čísla. Proto potřebujeme od množiny všech čísel ve tvaru součtu tří čtverců celých čísel odebrat taková čísla, která lze vyjádřit jen jako pouhé dva čtverce celých čísel.

Poznámka 3.1 Problémem by samozřejmě mohla být i čísla, která jsou sama druhou mocninou, ta jsou však podmnožinou množiny čísel ve tvaru součtu dvou čtverců.

Pozorný čtenář si jistě mohl povšimnout, že některá čísla, vyjádřitelná jako součet dvou druhých mocnin celých čísel, se dají zapsat i jako součet tří druhých mocnin přirozených čísel. Například číslo 29 lze zapsat jak ve tvaru $29 = 5^2 + 2^2$, tak i jako $29 = 4^2 + 3^2 + 2^2$. Proto bychom odebráním všech dvoučtvercových čísel z množiny tříčtvercových odebrali i některé možné hladiny energií. Nicméně, v Kapitole 4 využijeme vlastností množin, jimiž se budeme zabývat nyní, pro určení asymptotické hustoty spektra. Jak uvidíme, výsledek nebude nijak ovlivněn faktem, zda odebereme všechna čísla ve tvaru součtu dvou druhých mocnin celých čísel, či pouze jejich část.

Ukažme si tedy, která čísla lze vyjádřit jako součet dvou druhých mocnin celých čísel. K tomu budeme potřebovat tři pomocné poznatky:

Věta 3.1 *Nechť p je prvočíslo a $a, b \in \mathbb{Z}$ takové, že $\gcd(p, a) = \gcd(p, b) = 1$ a $p|(a^2 + b^2)$. Potom p je součtem dvou druhých mocnin celých čísel.*

Důkaz. Označme $n = a^2 + b^2 \ \ (a, b \in \mathbb{Z})$ nejmenší celé číslo, splňující $\gcd(p, a) = \gcd(p, b) = 1$ a $p|n$. Potom $n = mp, \ m \in \mathbb{N}$. Sestrojme čísla α, β taková, že $a \equiv \alpha (\mathrm{mod}\ p), \ b \equiv \beta (\mathrm{mod}\ p)$, přičemž $|\alpha|, |\beta| \leq \frac{p}{2}$. Pak vidíme, že

$$a^2 + b^2 \equiv \alpha^2 + \beta^2 \equiv 0 (\mathrm{mod}\ p),$$

z čehož vyplývá

$$mp = n = a^2 + b^2 \leq \alpha^2 + \beta^2 < p^2,$$

odtud $m < p$. Abychom důkaz dokončili, stačí ukázat, že $m = 1$. Uvažme pro spor situaci $1 < m < p$. Nyní sestrojme taková čísla a_1, a_2, že $a \equiv a_1 (\mathrm{mod}\ m), \ b \equiv b_1 (\mathrm{mod}\ m)$, přičemž

$|a_1|, |b_1| \leq \frac{m}{2}$. Z toho podobně jako v předchozím případě plyne, že

$$a_1^2 + b_1^2 \equiv a^2 + b^2 \equiv 0 (\text{mod } m)$$
$$a_1^2 + b_1^2 = um,\ u < m,$$

s tím, že u se nemůže rovnat 0, neboť pak by muselo nastat $a = xm,\ b = ym,\ x, y \in \mathbb{Z}$, tudíž $n = (x^2 + y^2)m^2 = mp$ a tedy $m|p$, což je nemožné, neboť $1 < m < p$. Proto $u \geq 1$.

Nyní uvažme, že součin každých dvou čísel, vyjádřitelných jako součet dvou čtverců, je opět součtem dvou čtverců. Skutečně

$$\begin{aligned} (a^2 + b^2) \cdot (a_1^2 + b_1^2) &= a^2 a_1^2 + b^2 b_1^2 + a_1^2 b^2 + a^2 b_1^2 = \\ &= (aa_1 + bb_1)^2 - 2aa_1 bb_1 + (a_1 b - ab_1)^2 + 2a_1 bab_1 = \\ &= (aa_1 + bb_1)^2 + (a_1 b - ab_1)^2. \end{aligned} \tag{3.1}$$

Protože $0 \equiv a^2 + b^2 \equiv aa_1 + bb_1 \equiv a_1 b - ab_1 (\text{mod } m)$, dostáváme

$$\begin{aligned} (a^2 + b^2) \cdot (a_1^2 + b_1^2) &= (\delta_1 m)^2 + (\delta_2 m)^2 \\ mp \cdot um &= m^2(\delta_1^2 + \delta_2^2) \\ up &= \delta_1^2 + \delta_2^2. \end{aligned} \tag{3.2}$$

Kvůli $u \geq 1$ je alepoň jedno z čísel δ_1, δ_2 různé od 0. Pokud by p dělilo obě z čísel δ_1, δ_2 dostali bychom $\delta_1^2 + \delta_2^2 > p^2$, což je však ve sporu s $u < m < p$. Tzn., že alespoň jedno z čísel δ_1, δ_2 není dělitelné p, což však znamená, že jím není dělitelné ani jedno (pokud by jen $\delta_1 = cp$, pak $up = c^2 p^2 + \delta_2^2$, tedy $u = c^2 p + \frac{\delta_2^2}{p}$, a to nelze, neboť určitě $\frac{\delta_2^2}{p} \notin \mathbb{Z}$; obdobně naopak). Tedy $\gcd(p, \delta_1) = \gcd(p, \delta_2) = 1$. Z definice čísla n by pak vyplynulo $mp \leq up$, což je opět spor s $u < m$. Proto není možné, aby $1 < m < p$, a tak $m = 1$. ∎

Věta 3.2 *Každé prvočíslo p ve tvaru $p = 4k + 1,\ k \in \mathbb{Z}$ lze jednoznačně vyjádřit jako součet dvou druhých mocnin celých čísel.*

Důkaz. Pro zadané p lze ukázat, že existuje takové $x \in \mathbb{Z}$, že $\gcd(p, x) = 1$ a zároveň $x^2 + 1 \equiv 0 (\text{mod } p)$[3]. Jelikož navíc $\gcd(p, 1) = 1$ a $p|(x^2 + 1^2)$, pak je podle Věty 3.1 p možno vyjádřit ve tvaru dvou čtverců.

[3] Plyne z vlastností Legendreova symbolu, viz [4].

Nyní předpokládejme, že pro různé dvojice čísel platí $p = a^2 + b^2 = c^2 + d^2$. Pak platí

$$p^2 = (a^2 + b^2) \cdot (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad + bc)^2 \tag{3.3}$$

$$\begin{aligned} (ac + bd) \cdot (ad + bc) &= a^2cd + abc^2 + abd^2 + b^2cd = \\ &= (a^2 + b^2)cd + (c^2 + d^2)^2ab = p(ab + cd). \end{aligned} \tag{3.4}$$

Tudíž buď $p|(ac+bd)$, nebo $p|(ad+bc)$. V prvním případě by to však znamenalo $(ac+bd)^2 \geq p^2$, takže s přihlédnutím ke vztahu (3.3) by muselo platit $ad = bc$. Uvážíme-li, že $\gcd(c, d) \mid (c^2 + d^2) = p$, pak je $\gcd(c, d)$ roven buď 1, nebo p, pokud by však byl roven p, dostaneme spor

$$p = c^2 + d^2 \geq 2p^2.$$

Proto $\gcd(c, d) = 1$, tedy $c|a$, stejně tak $\gcd(a, b) = 1$, ergo $a|c$, z čehož plyne $a = c$ a tedy i $b = d$. Analogicky u druhého případu. ∎

Věta 3.3 *Jestliže pro přirozené číslo n platí $n = 4k + 3,\ k \in \mathbb{Z}_0^+$, pak n nelze vyjádřit ve tvaru $n = a^2 + b^2,\ a, b \in \mathbb{Z}$.*

Důkaz. Pro zadané n platí $n \equiv 3 (\mathrm{mod}\ 4)$. Postupujme systematicky:

1. Obě čísla a, b jsou sudá. Potom platí

$$a^2 + b^2 = (2x)^2 + (2y)^2 = 4(x^2 + y^2) \equiv 0 (\mathrm{mod}\ 4).$$

2. Jedno z čísel a, b je liché (např. a).

$$a^2 + b^2 = (2x + 1)^2 + (2y)^2 = 4(x^2 + y^2 + x) + 1 \equiv 1 (\mathrm{mod}\ 4).$$

3. Obě čísla a, b jsou lichá.

$$a^2 + b^2 = (2x + 1)^2 + (2y + 1)^2 = 4(x^2 + y^2 + x + y) + 2 \equiv 2 (\mathrm{mod}\ 4).$$

Jiné možnosti nejsou a tak nemůže nastat $a^2 + b^2 \equiv 3 (\mathrm{mod}\ 4)$. ∎

Nyní můžeme konečně nabyté poznatky použít pro důkaz, která přirozená čísla lze vyjádřit jako součet dvou celočíselných čtverců.

Věta 3.4 *Přirozené číslo $n > 1$ lze vyjádřit ve tvaru $n = a^2 + b^2,\ a, b \in \mathbb{Z}$ právě tehdy, když kanonický rozklad čísla n neobsahuje číslo $p_i^{\alpha_i}$ takové, že prvočíslo $p_i = 4k + 3$ a $\alpha_i = 2m + 1$, $k, m \in \mathbb{Z}_0^+$.*

Důkaz. Nejprve vezměme číslo $n = a^2 + b^2,\ a, b \in \mathbb{Z}$. Nechť $\gcd(a, b) = d$, pak $a = da_1,\ b = db_2$, kde $\gcd(a_1, b_1) = 1$ a tedy

$$n = d^2(a_1^2 + b_1^2). \tag{3.5}$$

Předpokládejme, že p je prvočíslo ve tvaru $p = 4k + 3$ a platí $p|n$. Pokud $p \nmid (a_1^2 + b_1^2)$, pak s ohledem na 3.5 musí vystupovat v kanonickém rozkladu čísla n se sudou mocninou. Pokud by naopak $p|(a_1^2+b_1^2)$, pak by buď muselo p dělit obě čísla a_1, b_1, tedy opět být v kanonickém rozkladu čísla n se sudou mocninou, anebo v opačném případě by platilo $\gcd(a_1, p) = \gcd(b_1, p) = 1$, což by s ohledem na Větu 3.1 znamenalo, že p je součtem dvou čtverců. To je však ve sporu s Větou 3.3.

Nyní dokážeme implikaci druhým směrem. Nechť $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ je kanonický rozklad čísla n a předpokládejme, že pro každé prvočíslo ve tvaru $p = 4k + 3$ platí buď $p \nmid n$, nebo že příslušný exponent je sudý. Dále přepišme exponenty v rozkladu jako $\alpha_i = 2\beta_i + \gamma_i$, přičemž $\forall i \in \{1, 2, \dots, m\} : \beta_i \in \mathbb{Z}_0^+,\ \gamma_i \in \{0, 1\}$. Odtud

$$n = \left(p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}\right)^2 p_1^{\gamma_1} p_2^{\gamma_2} \dots p_m^{\gamma_m} = P^2 q_1 q_2 \dots q_s,$$

kde $P = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m}$ a $q_1, q_2, \dots, q_s$ jsou ta prvočísla, pro něž $\gamma_i = 1$. Pak z předpokladu $q_i = 4k + 1,\ i \in \{1, 2, \dots, s\}$ víme díky Větě 3.2, že každé z pročísel $q_1, q_2, \dots, q_s$ lze vyjádřit jako součet dvou druhých mocnin celých čísel. Jistě můžeme zapsat $P^2 = P^2 + 0^2$ a na základě vztahu (3.1) platí, že součin čísel ve tvaru dvou čtverců je opět součtem dvou čtverců, proto tohoto tvaru nabývá i n. ∎

3.2 Přirozená čísla ve tvaru součtu tří druhých mocnin celých čísel

Naším dalším a hlavním krokem při honbě za energetickým spektrem částice v potenciálové jámě bude objasnění, jaká přirozená čísla lze vyjádřit jako součet tří druhých mocnin celých čísel. Dokážeme nutnou podmínku toho, aby přirozené číslo tohoto tvaru nabývalo, s odkazem na literaturu pak uvedeme, že se jedná i o podmínku postačující.

Věta 3.5 *Jestliže přirozené číslo $n > 1$ lze vyjádřit ve tvaru součtu tří druhých mocnin celých čísel, potom n nelze zapsat ve tvaru $n = 4^j(8k + 7)$, kde $j, k \in \mathbb{Z}_0^+$.*

Důkaz. Nejprve uvažme speciální případ, kdy $j = 0$. Tedy ukážeme, že pokud $n = a^2 + b^2 + c^2$, kde $a, b, c \in \mathbb{Z}$, tak platí $n \neq 8k + 7$, kde $k \in \mathbb{Z}_0^+$. Pak máme čtyři možnosti:

1. Čísla a, b, c jsou sudá. Potom existují celá čísla k_1, k_2, k_3 taková, že

$$n = (2k_1)^2 + (2k_2)^2 + (2k_3)^2 = 4(k_1^2 + k_2^2 + k_3^2).$$

Pak $n \equiv 0 (\mathrm{mod}\ 4)$, zatímco $8k + 7 \equiv 3 (\mathrm{mod}\ 4)$, tudíž $n \neq 8k + 7$.

2. Jedno z čísel a, b, c je liché a dvě jsou sudá. Potom existují celá čísla k_1, k_2, k_3 taková, že

$$n = (2k_1 + 1)^2 + (2k_2)^2 + (2k_3)^2 = 4(k_1^2 + k_2^2 + k_3^2 + k_1) + 1.$$

   V tomto případě tedy $n \equiv 1 (\mathrm{mod}\ 4)$, zatímco $8k + 7 \equiv 3 (\mathrm{mod}\ 4)$, a tak $n \neq 8k + 7$.

3. Jedno z čísel a, b, c je sudé a dvě jsou lichá. Potom existují celá čísla k_1, k_2, k_3 taková, že

$$n = (2k_1 + 1)^2 + (2k_2 + 1)^2 + (2k_3)^2 = 4(k_1^2 + k_2^2 + k_3^2 + k_1 + k_2) + 2.$$

   Vidíme, že $n \equiv 2 (\mathrm{mod}\ 4)$, zatímco $8k + 7 \equiv 3 (\mathrm{mod}\ 4)$, tudíž opět $n \neq 8k + 7$.

4. Všechna čísla a, b, c jsou lichá. Potom existují celá čísla k_1, k_2, k_3 taková, že

$$\begin{aligned} n &= (2k_1 + 1)^2 + (2k_2 + 1)^2 + (2k_3 + 1)^2 \\ n &= 4(k_1(k_1 + 1) + k_2(k_2 + 1) + k_3(k_3 + 1)) + 3 \\ n &= 8(t + u + v) + 3. \end{aligned}$$

   Tady dostáváme, že $n \equiv 3 (\mathrm{mod}\ 8)$, zatímco $8k + 7 \equiv 7 (\mathrm{mod}\ 8)$, takže i v tomto případě $n \neq 8k + 7$.

Z předchozího je patrné, že za všech okolností pro každé číslo $n = a^2 + b^2 + c^2$, kde $a, b, c \in \mathbb{Z}$, platí $n \neq 8k + 7$, $k \in \mathbb{Z}_0^+$.

Nyní sporem ukážeme, že pokud $n = a^2 + b^2 + c^2$, kde $a, b, c \in \mathbb{Z}$, tak platí $n \neq 4^j(8k + 7)$, kde $j, k \in \mathbb{Z}_0^+$. Předpokládejme tedy, že $n_0 = 4^{j_0}(8k_0 + 7)$, je nejmenší přirozené číslo takové, že existují $a, b, c, j, k \in \mathbb{Z}_0^+$ taková, aby platilo $n = a^2 + b^2 + c^2 = 4^j(8k + 7)$. Z předpokladu plyne, že $n_0 \equiv 0 (\mathrm{mod}\ 4)$ a to nastane pouze v případě, že všechna čísla a, b, c jsou sudá. Proto

$$\begin{gathered} n_0 = (2k_1)^2 + (2k_2)^2 + (2k_3)^2 = 4(k_1^2 + k_2^2 + k_3^2) = 4^{j_0}(8k_0 + 7) \\ \frac{n_0}{4} = n^* = k_1^2 + k_2^2 + k_3^2 = 4^{j_0 - 1}(8k_0 + 7), \end{gathered}$$

což je však ve sporu s předpokládanou minimalitou čísla n_0. ∎

Věta 3.5 představuje implikaci jedním směrem, dá se však dokázat také opačná implikace.

Věta 3.6 *Jestliže pro přirozené číslo $n > 1$ platí, že jej nelze zapsat ve tvaru $n = 4^j(8k + 7)$, kde $j, k \in \mathbb{Z}_0^+$, potom jej lze vyjádřit ve tvaru součtu tří druhých mocnin celých čísel.*

Důkaz. Důkaz této věty pro jeho složitost neuvádíme, jsou při něm využity poznatky z oblasti kvadratických kongruencí, aritmetických funkcí a lineární algebry. Zájemci mohou důkaz nalézt například v [12]. ∎

Spojením Vět 3.5 a 3.6 dostáváme větu, jež plně vypovídá o tom, která čísla lze vyjádřit jako součet tří druhých mocnin celých čísel.

Věta 3.7 (Legendreova) *Přirozené číslo $n > 1$ lze vyjádřit jako součet tří druhých mocnin celých čísel právě tehdy, když číslo n nelze zapsat ve tvaru $n = 4^j(8k + 7)$, kde $j, k \in \mathbb{Z}_0^+$.*

Všimněme si, že přímým důsledkem věty 3.7 je následující fakt:
Mějme množiny A a B_3, přičemž

$$A = \{4^j(8k + 7) \mid j, k \in \mathbb{Z}_0^+\}$$
$$B_3 = \{a^2 + b^2 + c^2 > 0 \mid a, b, c \in \mathbb{Z}\}.$$

Potom na základě Věty 3.7 a zjevné skutečnosti, že $1 \notin A$ a zároveň $1 \in B_3$, platí, že $A \cap B_3 = \emptyset$, a zároveň $A \cup B_3 = \mathbb{N}$.

Poznámka 3.2 Dohodněme se, že množinu všech přirozených čísel, vyjádřitelných ve tvaru součtu tří druhých mocnin celých čísel budeme pro jednoduchost i ve zbytku práce značit B_3, stejně tak množinu čísel ve tvaru součtu dvou druhých mocnin celých čísel budeme značit B_2.

3.3 Lagrangeova věta o čtyřech čtvercích

Otázku součtu dvou i tří druhých mocnin, jíž jsme se zabývali kvůli energii částice, jsme tedy vyřešili. S ohledem na další pozorování nám může být prospěšná úvaha o tom, jak by situace vypadala pro součet čtyř čtverců celých čísel. Tento problém vyřešil v roce 1770 Joseph Lagrange, který dokázal, že čtyři čtverce již stačí na vyjádření jakéhokoliv přirozeného čísla.

Věta 3.8 (Lagrangeova) *Každé přirozené číslo n lze vyjádřit ve tvaru $n = a^2 + b^2 + c^2 + d^2$, kde $a, b, c, d \in \mathbb{Z}$.*

Důkaz. Ze všeho nejdříve uvažme tzv. Eulerovu identitu:

$$\begin{aligned}(a_1^2 + b_1^2 + c_1^2 + d_1^2) \cdot (a_2^2 + b_2^2 + c_2^2 + d_2^2) = \\ = (a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 + (a_1b_2 - b_1a_2 + c_1d_2 - d_1c_2)^2 + \\ +(a_1c_2 - b_1d_2 - c_1a_2 + d_1b_2)^2 + (a_1d_2 + b_1c_2 - c_1b_2 - d_1a_2)^2. \qquad (3.6)\end{aligned}$$

O platnosti tohoto vztahu se lze přesvědčit přímým roznásobením. Mimo jiné nám tato identita říká, že pokud mezi sebou vynásobíme čísla, jež jsou součtem čtyř druhých mocnin, pak opět dostaneme součet čtyř druhých mocnin. To by však znamenalo, že pokud by každé prvočíslo bylo možné vyjádřit jako součet čtyř čtverců, pak by to zákonitě platilo i pro všechna čísla složená, a tak stačí větu dokázat pro prvočísla a číslo 1.

Nejprve ukažme, že pro každé prvočíslo $p > 2$ platí, že jestliže p dělí nějaké $a^2 + b^2 + c^2 + d^2$ a zároveň alespoň jedno z čísel a, b, c, d nedělí, pak je samo p součtem čtyř čtverců. Nechť

$n_0 = a^2 + b^2 + c^2 + d^2$ je nejmenší takové číslo, pro které platí $n_0 = kp$ a bez újmy na obecnosti například $p \nmid a$. Nyní uvažme čísla $\alpha, \beta, \gamma, \delta$ taková, že

$$\begin{aligned} a &\equiv \alpha (\mathrm{mod}\ p) \\ b &\equiv \beta (\mathrm{mod}\ p) \\ c &\equiv \gamma (\mathrm{mod}\ p) \\ d &\equiv \delta (\mathrm{mod}\ p) \\ |\alpha|, |\beta|, |\gamma|, |\delta| &< \frac{p}{2}. \end{aligned}$$

Potom zjevně platí, že

$$n_0 = kp \equiv \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 (\mathrm{mod}\ p).$$

Z minimality n_0 a předpokladu (3.3) vyplývá, že $kp = n_0 \leq \alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4\frac{p^2}{4} = p^2$, což nás vede k tomu, že $1 \leq k < p$. Abychom se dobrali toho, že p je součtem čtyř čtverců, stačí dokázat, že $k = 1$. Položme nyní $1 < k < p$ a čísla a_1, b_1, c_1, d_1 následovně:

$$\begin{aligned} a &\equiv a_1 (\mathrm{mod}\ k) \\ b &\equiv b_1 (\mathrm{mod}\ k) \\ c &\equiv c_1 (\mathrm{mod}\ k) \\ d &\equiv d_1 (\mathrm{mod}\ k) \\ |a_1|, |b_1|, |c_1|, |d_1| &\leq \frac{k}{2}, \end{aligned} \tag{3.7}$$

odtud $a_1^2 + b_1^2 + c_1^2 + d_1^2 = sk,\ s \geq 0$. Pokud by bylo $s = 0$, pak by muselo platit $a_1 = b_1 = c_1 = d_1 = 0$. To by znamenalo, že k dělí každé z čísel a, b, c, d a tedy $k^2 \mid (a^2 + b^2 + c^2 + d^2) = kp$, potom by však platilo, že $k \mid p$, což není možné, neboť $1 < k < p$ a tak $s \geq 1$.

Nyní si naopak představme, že $|a_1| = |b_1| = |c_1| = |d_1| = \frac{k}{2}$. To by mohlo nastat pouze při sudém k, tedy k lze zapsat jako $k = 2q,\ q \in \mathbb{Z}$. Vyjádříme-li a, zjistíme, že

$$a = a_1 + kt_1 = \pm\frac{2q}{2} + 2qt_1 = q(2t_1 \pm 1),$$

analogicky $b = q(2t_2 \pm 1),\ c = q(2t_3 \pm 1),\ d = q(2t_4 \pm 1)$, přičemž čísla $(2t_i \pm 1),\ i \in \{1, 2, 3, 4\}$

jsou lichá. Tato situace ale vede ke sporu, neboť nemůže nastat

$$n_0 = 2qp = q^2\left((2t_1 \pm 1)^2 + (2t_2 \pm 1)^2 + (2t_3 \pm 1)^2 + (2t_4 \pm 1)^2\right)$$
$$2p = q(4t_1^2 \pm 4t_1 + 1 + 4t_2^2 \pm 4t_2 + 1 + 4t_3^2 \pm 4t_3 + 1 + 4t_4^2 \pm 4t_4 + 1)$$
$$p = 2q(t_1^2 \pm t_1 + t_2^2 \pm t_2 + t_3^2 \pm t_3 + t_4^2 \pm t_4 + 1),$$

a to z toho důvodu, že by muselo platit $2 \mid p$, což by bylo možné pouze pro sudé p. Z definice víme, že $p > 2$ (číslo 2 je jediné sudé prvočíslo). Proto alespoň jedno z čísel $|a_1|, |b_1|, |c_1|, |d_1|$ je ostře menší, než $\frac{k}{2}$, a tudíž $s < k$.

Teď aplikujme na čísla sk a kp vztah (3.6). Dostaneme

$$sk \cdot kp = (a_1^2 + b_1^2 + c_1^2 + d_1^2) \cdot (a^2 + b^2 + c^2 + d^2) =$$
$$= (a_1a + b_1b + c_1c + d_1d)^2 + (a_1b - b_1a + c_1d - d_1c)^2 +$$
$$+(a_1c - b_1d - c_1a + d_1b)^2 + (a_1d + b_1c - c_1b - d_1a)^2.$$

Pojďme se nyní podívat na každou ze závorek na pravé straně zvlášť. Z předpokladu (3.7) vidíme, že $a = q_1k + a_1,\ b = q_2k + b_1,\ c = q_3k + c_1,\ d = q_4k + d_1$, kde $q_1, q_2, q_3, q_4 \in \mathbb{Z}$. Pro členy v závorkách to znamená následující:

1.

$$\begin{aligned}
(a_1a + b_1b + c_1c + d_1d)^2 &= (a_1(q_1k + a_1) + b_1(q_2k + b_1) + c_1(q_3k + c_1) + d_1(q_4k + d_1))^2 \\
&= \left(k(a_1q_1 + b_1q_2 + c_1q_3 + d_1q_4) + a_1^2 + b_1^2 + c_1^2 + d_1^2\right)^2 \\
&= (k(a_1q_1 + b_1q_2 + c_1q_3 + d_1q_4) + sk)^2 \\
&= (k(\underbrace{a_1q_1 + b_1q_2 + c_1q_3 + d_1q_4 + s}_{=\,\xi_1\,\in\,\mathbb{Z}}))^2.
\end{aligned}$$

2.

$$\begin{aligned}
(a_1b - b_1a + c_1d - d_1c)^2 &= (a_1(q_2k + b_1) - b_1(q_1k + a_1) + c_1(q_4k + d_1) - d_1(q_3k + c_1))^2 \\
&= (k(a_1q_2 - b_1q_1 + c_1q_4 - d_1q_3) + a_1b_1 - b_1a_1 + c_1d_1 - d_1c_1)^2 \\
&= (k(\underbrace{a_1q_2 - b_1q_1 + c_1q_4 - d_1q_3}_{=\,\xi_2\,\in\,\mathbb{Z}}))^2.
\end{aligned}$$

3.

$$\begin{aligned}(a_1c - b_1d - c_1a + d_1b)^2 &= (a_1(q_3k + c_1) - b_1(q_4k + d_1) - c_1(q_1k + a_1) + d_1(q_2k + b_1))^2 \\ &= (k(a_1q_3 - b_1q_4 - c_1q_1 + d_1q_2) + a_1c_1 - b_1d_1 - c_1a_1 + d_1b_1)^2 \\ &= (k(\underbrace{a_1q_3 - b_1q_4 - c_1q_1 + d_1q_2}_{=\,\xi_3\,\in\,\mathbb{Z}}))^2.\end{aligned}$$

4.

$$\begin{aligned}(a_1d + b_1c - c_1b - d_1a)^2 &= (a_1(q_4k + d_1) + b_1(q_3k + c_1) - c_1(q_2k + b_1) - d_1(q_1k + a_1))^2 \\ &= (k(a_1q_4 + b_1q_3 - c_1q_2 - d_1q_1) + a_1d_1 + b_1c_1 - c_1b_1 - d_1a_1)^2 \\ &= (k(\underbrace{a_1q_4 + b_1q_3 - c_1q_2 - d_1q_1}_{=\,\xi_4\,\in\,\mathbb{Z}}))^2.\end{aligned}$$

Teď již můžeme pokračovat v původní myšlence:

$$\begin{aligned}sk \cdot kp &= (k\xi_1)^2 + (k\xi_2)^2 + (k\xi_3)^2 + (k\xi_4)^2 \\ k^2sp &= k^2(\xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2) \\ sp &= \xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2.\end{aligned} \tag{3.8}$$

Jelikož víme, že $sp \neq 0$, musí být alespoň jedno z čísel ξ_i nenulové. Pokud p dělí všechna čísla ξ_i, pak nastane $sp = \xi_1^2 + \xi_2^2 + \xi_3^2 + \xi_4^2 \geq p^2$, odtud $s \geq p$, což je však ve sporu s dříve ukázaným $s < k < p$. Alespoň pro jedno z čísel ξ_i tedy platí $p \nmid \xi_i$. Pak by ovšem muselo být splněno $n_0 = kp \leq sp$, což je opět ve sporu s $s < k$. Vidíme tedy, že předpoklad $1 < k < p$ nemůže platit, a proto $k = 1$.

Pomocí výše zjištěného teď dokážeme, že každé prvočíslo p je součtem čtyř čtverců. Mějme množinu

$$M_1 = \left\{1 + 0^2, 1 + 1^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}.$$

Nyní sporem ukážeme, že každé dva prvky množiny M_1 jsou vzájemně inkongruentní modulo p. Nechť $u, v \in \mathbb{Z}$ jsou taková čísla, že $|u|, |v| \in \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$, $|u| \neq |v|$ a předpokládejme, že $1 + u^2 \equiv 1 + v^2 (\mathrm{mod}\ p)$. Potom $p \mid (u - v)(u + v)$. Za tohoto předpokladu by p dělilo aspoň jedno z čísel $(u - v), (u + v)$, což vede ke sporu, jelikož $1 \leq |u \pm v| \leq p - 1$ a tudíž musí platit, že každé 2 různé prvky množiny M_1 jsou vzájemně inkongruentní modulo p. Totéž bude platit pro prvky množiny

$$M_2 = \left\{0^2, -1^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}.$$

Množiny $M_1,\ M_2$ jsou evidentně disjunktní, sjednocením obou množin pak dostáváme množinu M, pro kterou platí $|M| = 2\left(\frac{p-1}{2}+1\right) = p+1$. Jinými slovy určitě existuje alespoň jedna dvojice čísel $x, y \in \mathbb{Z}$, splňující následující podmínky:

$$1 + x^2 \in M_1$$
$$-y^2 \in M_2$$
$$1 + x^2 \equiv -y^2 (\text{mod } p).$$

Díky existenci takových x, y tedy můžeme psát $0^2+1^2+x^2+y^2 \equiv 0(\text{mod } p)$, takže $p \mid (0^2+1^2+x^2+y^2)$, přičemž $p \nmid 1$. Pro tyto situace jsme již dokázali, že p je součtem čtyř čtverců, a proto je každé prvočíslo $p > 2$ součtem čtyř čtverců. Očividně platí $1 = 1^2+0^2+0^2+0^2$, stejně tak $2 = 1^2+1^2+0^2+0^2$ a na základě Eulerovy identity můžeme říct, že věta platí i pro všechna čísla složená. Jelikož žádná jiná přirozená čísla, než 1, prvočísla a čísla složená neexistují, věta skutečně platí. ∎

4 Asymptotická hustota

V této kapitole se zamyslíme nad otázkou, jaké zastoupení mají čísla, odpovídající kvantovým stavům částice v potenciálové jámě, mezi přirozenými čísly. Spočítat pouhým podílem relativní četnost v tomto případě nemá smysl, neboť jak množina kvantových stavů, tak množina přirozených čísel jsou (spočetně) nekonečné. Poněkud sofistikovanějším nástrojem pro porovnávání velikostí množin v oboru přirozených čísel je právě asymptotická hustota.

4.1 Definice, základní vlastnosti

Definice 4.1 *Nechť $A \subseteq \mathbb{N}$. **Horní**, resp. **dolní asymptotickou hustotou** množiny A nazýváme číslo*

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{A(n)}{n},$$

resp.

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n},$$

přičemž $A(n)$ označuje počet prvků množiny A, nepřesahujících číslo n. Pokud navíc platí $\overline{d}(A) = \underline{d}(A)$, potom číslo

$$d(A) = \overline{d}(A) = \underline{d}(A) = \lim_{n\to\infty} \frac{A(n)}{n}$$

*označujeme jako **asymptotickou hustotu** množiny A.*

Už na základě definice můžeme o asymptotické hustotě mnohé zjistit. Především skutečnost, že horní i dolní asymptotická hustota vždy existují, avšak asymptotická hustota existovat nemusí (limes superior i limes inferior posloupnosti vždy existují, ale nemusí existovat její limita). Jinými slovy, asymptotická hustota množiny existuje, existuje-li příslušná limita. Některé další vlastnosti asymptotické hustoty shrnuje následující věta:

Věta 4.1 *Nechť $A \subseteq \mathbb{N}$. Potom platí:*

1. $d(\mathbb{N}) = 1$.
2. $0 \leq \underline{d}(A) \leq \overline{d}(A) \leq 1$.
3. *Nechť $K \subseteq \mathbb{N}$ a $|K| < \infty$. Jestliže $d(A)$ existuje, pak platí, že $d(A \cup K) = d(A - K) = d(A)$.*
4. *Nechť $D \subseteq \mathbb{N}$, $A \cap D = \emptyset$ a $A \cup D = \Omega$. Jestliže existují $d(\Omega)$ a $d(D)$, pak platí, že $d(A) = d(\Omega) - d(D)$.*
5. *Nechť $D \subseteq \mathbb{N}$ je množina taková, že $A = \mathbb{N} - D$. Pokud existuje $d(D)$, pak pro asymptotickou hustotu množiny A platí $d(A) = 1 - d(D)$.*
6. *Nechť $A \subseteq B \subseteq \mathbb{N}$ a existuje $d(B)$. Potom platí, že $0 \leq \underline{d}(A) \leq \overline{d}(A) \leq d(B) \leq 1$.*

Důkaz.

1. Zjevně platí $\mathbb{N}(n) = n$, a tedy $\lim_{n\to\infty} \frac{\mathbb{N}(n)}{n} = \lim_{n\to\infty} \frac{n}{n} = 1$.

2. Počet prvků množiny A, nepřesahujících číslo n, nemůže být větší, než n, ani menší, než 0. Proto

$$0 \leq \frac{A(n)}{n} \leq \frac{n}{n} = 1$$
$$0 \leq \liminf_{n\to\infty} \frac{A(n)}{n} \leq \limsup_{n\to\infty} \frac{A(n)}{n} \leq 1.$$

3. Množina K je konečná, tudíž $|K| = k, k \in \mathbb{N}$. Pro dostatečně velká n pak jistě platí

$$A(n) \leq (A \cup K)(n) \leq A(n) + k$$
$$A(n) \geq (A - K)(n) \geq A(n) - k,$$

   díky čemuž s využitím věty o limitě sevřené posloupnosti dostaneme

$$\begin{array}{ccccccc} \lim\limits_{n\to\infty} \frac{A(n)}{n} & \leq & \liminf\limits_{n\to\infty} \frac{(A\cup K)(n)}{n} & \leq & \limsup\limits_{n\to\infty} \frac{(A\cup K)(n)}{n} & \leq & \lim\limits_{n\to\infty} \frac{A(n)+k}{n} \\ d(A) & \leq & \underline{d}(A \cup K) & \leq & \overline{d}(A \cup K) & \leq & d(A), \end{array}$$

   a proto $d(A \cup K) = d(A)$, analogicky pro $d(A - K)$.

4. Z definovaných vlastností množin A, D, Ω plyne $\Omega(n) = (A \cup D)(n) = A(n) + D(n)$. Odtud $A(n) = \Omega(n) - D(n)$, čili

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} \frac{\Omega(n)}{n} - \lim_{n\to\infty} \frac{D(n)}{n} = d(\Omega) - d(D).$$

5. Plyne z bodů 1 a 4: Pokud za množinu Ω z bodu 4 dosadíme $\mathbb{N}$, dostáváme

$$d(A) = d(\mathbb{N}) - d(D) = 1 - d(D).$$

6. Fakt, že $0 \leq \underline{d}(A) \leq \overline{d}(A)$ plyne hned z bodu 2, stejně jako $d(B) \leq 1$, proto stačí ukázat, že $\overline{d}(A) \leq d(B)$. Vzhledem k tomu, že $A \subseteq B$, tak musí platit $A(n) \leq B(n)$, potažmo $\frac{A(n)}{n} \leq \frac{B(n)}{n}$. Jelikož $d(B) = \lim_{n\to\infty} \frac{B(n)}{n}$, pak takových $\frac{B(n)}{n}$, větších než $d(B)+\varepsilon$, $\varepsilon \in \mathbb{R}^+$ je pouze konečně mnoho. Uvažujme situaci, že by $\overline{d}(A) > d(B)$. Položíme-li $\varepsilon = \frac{1}{2}(\overline{d}(A) - d(B)$, pak bude existovat nekonečně mnoho $\frac{A(n)}{n}$, větších než $d(B)+\varepsilon$. Protože $\frac{A(n)}{n} \leq \frac{B(n)}{n}$, muselo by být i nekonečně mnoho takových $n \in \mathbb{N}$, pro která platí $\frac{B(n)}{n} \geq d(B) + \varepsilon$, což vede ke sporu.

■

Dříve, než přistoupíme ke složitějšímu výpočtu asymptotické hustoty spektra, ukažme si pro názornost několik příkladů.

Příklad 1

Například množina kladných prvků zbytkové třídy $\overline{3}(\mathrm{mod}\ 5)$ má asymptotickou hustotu $\frac{1}{5}$. Proč? Zadaná množina se dá vyjádřit ve tvaru $Z = \{5q - 2 \mid q \in \mathbb{N}\}$. $Z(n)$ potom určíme jako počet všech q, pro která platí, že $5q-2 \leq n$. Pokud bychom se na situaci podívali podrobněji, zjišťujeme, že

$$\begin{aligned} 5q &\leq n+2 \\ q &\leq \tfrac{n+2}{5}. \end{aligned}$$

Jelikož q je celé číslo, je zjevné, že počet všech vyhovujících q odpovídá celé části čísla $\frac{n+2}{5}$. Odtud $Z(n) = \left[\frac{n+2}{5}\right] = \frac{n+2}{5} - \varepsilon_n$, kde $\varepsilon_n \in \langle 0, 1)$. Nyní už jen stačí dosadit do příslušné limity, čímž vzniká

$$d(Z) = \lim_{n\to\infty} \frac{Z(n)}{n} = \lim_{n\to\infty} \frac{\frac{n+2}{5} - \varepsilon_n}{n} = \frac{1}{5}.$$

■

Příklad 2

Existují množiny, které nejsou konečné, ale jejich asymptotická hustota je rovna nule. Takovou množinou je například $M = \{ra^s \mid a \in \mathbb{N}\}$, kde r, s jsou přirozené konstanty a $s > 1$. Číslo $M(n)$ je totiž rovno $\left[\sqrt[s]{\frac{n}{r}}\right]$. Příslušná limita pak vypadá následovně:

$$d(M) = \lim_{n\to\infty} \frac{M(n)}{n} = \lim_{n\to\infty} \frac{\sqrt[s]{\frac{n}{r}}}{n} = \lim_{n\to\infty} \frac{1}{r^{\frac{1}{s}} n^{\frac{s-1}{s}}} = 0.$$

Dalším příkladem nekonečné množiny s nulovou asymptotickou hustotou může být kupříkladu množina všech prvočísel (plyne z prvočíselné věty, viz [4]). ■

Příklad 3

Jak jsme řekli, ne každá množina musí mít asymptotickou hustotu. Například množina $S = \{1, \ldots, 9, 100, \ldots, 999, 10000, \ldots\}$, čili množina všech přirozených čísel, jejichž dekadický zápis obsahuje lichý počet cifer. Obecně platí, že číslo $\alpha \cdot 10^\beta$, kde $\alpha \in \{1, \ldots, 9\}, \beta \in \mathbb{Z}_0^+$, má $\beta + 1$ cifer. Do naší množiny tedy patří všechna čísla ve tvaru $\alpha \cdot 10^\beta$ se sudým β.

Podívejme se nyní, čemu se rovná $S(5 \cdot 10^{2n+1})$. Pokud by bylo $n = 0$, pak by platilo, že $S(n) = 9$, v tomto rozsahu by totiž do množiny S patřila pouze čísla od 1 do 9. Pokud by bylo $n = 1$, pak $S(n) = 909$, neboť k původním devíti by se nyní přičetl počet všech čísel od 100 do 999, kterých je 900. Lze se snadno přesvědčit, že obecně platí

$$S(5 \cdot 10^{2n+1}) = 9 \cdot (1 + 10^2 + ... + 10^{2n}) = 9 \cdot \sum_{i=0}^{n} 10^{2i}.$$

Uvedený výraz se dá dále upravit, uvědomíme-li si, že se jedná o součet geometrické posloupnosti, jenž je dán vztahem $\sum_{j=0}^{n} a_j = a_0 \cdot \frac{1-q^{n+1}}{1-q}$, kde a_0 je počáteční člen posloupnosti a q je kvocient. V tomto případě $a_0 = 1$ a $q = 10^2$. Proto

$$S(5 \cdot 10^{2n+1}) = 9 \cdot 1 \cdot \frac{1 - 10^{2n+2}}{1 - 10^2} = \frac{10^{2n+2} - 1}{11}.$$

Nyní se pokusme určit $S(5 \cdot 10^{2n+2})$. Jelikož žádné z čísel od 10^{2n+1} do $10^{2n+2} - 1$ do množiny S nepatří a počet čísel od 10^{2n+2} do $5 \cdot 10^{2n+2}$ je roven $4 \cdot 10^{2n+2} + 1$, můžeme říci, že

$$S(5 \cdot 10^{2n+2}) = S(5 \cdot 10^{2n+1}) + 4 \cdot 10^{2n+2} + 1 = \frac{10^{2n+2} - 1}{11} + 4 \cdot 10^{2n+2} + 1 = \frac{45 \cdot 10^{2n+2} + 10}{11}.$$

Podívejme se, co by tyto výsledky znamenaly pro existenci příslušné limity. Pokud posloupnost konverguje, pak k témuž číslu konverguje i posloupnost z ní vybraná, tedy za předpokladu, že existuje $d(S)$ musí platit

$$d(S) = \lim_{n\to\infty} \frac{S(n)}{n} = \lim_{n\to\infty} \frac{S(5 \cdot 10^{2n+1})}{5 \cdot 10^{2n+1}} = \lim_{n\to\infty} \frac{S(5 \cdot 10^{2n+2})}{5 \cdot 10^{2n+2}},$$

opak je však pravdou:

$$\lim_{n\to\infty} \frac{S(5 \cdot 10^{2n+1})}{5 \cdot 10^{2n+1}} = \lim_{n\to\infty} \frac{\frac{10^{2n+2}-1}{11}}{5 \cdot 10^{2n+1}} = \frac{2}{11}$$
$$\lim_{n\to\infty} \frac{S(5 \cdot 10^{2n+2})}{5 \cdot 10^{2n+2}} = \lim_{n\to\infty} \frac{\frac{45 \cdot 10^{2n+2}+10}{11}}{5 \cdot 10^{2n+2}} = \frac{9}{11}.$$

Z výše uvedeného vyplývá, že $d(S)$ neexistuje. ∎

Příklad 4

Jako poslední příklad uveďme množinu nedegenerovaných hladin energií částice v potenciálové jámě. Na konci Kapitoly 2 jsme se zmínili o tom, že nedegenerované mohou být pouze ty hladiny, pro které nezáleží na uspořádání kvantových čísel, což zjevně platí pouze když $a = b = c$ a člen $a^2 + b^2 + c^2$ tak přechází ve $3a^2$. Zároveň to musí být taková $3a^2$, která nelze jiným způsobem vyjádřit jako součet tří druhých mocnin.

Označme B_n jako množinu nedegenerovaných hladin a $B^* = \{3a^2 \mid a \in \mathbb{N}\}$. Je evidentní, že $B_n \subseteq B^*$. Dále vidíme, že množina B^* je konkrétním případem množiny M z Příkladu 2, kde $r = 3$ a $s = 2$. Nyní již lze na základě 6. bodu Věty 4.1 určit $\overline{d}(B_n)$:

$$0 \leq \overline{d}(B_n) \leq d(B^*) = 0 \quad \Rightarrow \quad \overline{d}(B_n) = 0.$$

Nakonec na základě 2. bodu Věty 4.1 máme $0 \leq \underline{d}(B_n) \leq \overline{d}(B_n) = 0$, tudíž $d(B_n)$ existuje a je rovna 0. Proto lze říci, že nedegenerované hladiny teoreticky mají jen nepatrné zastoupení. ∎

4.2 Asymptotická hustota množiny B_2

Abychom mohli určit asymptotickou hustotu povolených energií, potřebujeme nejprve určit asymptotickou hustotu množiny B_2 (viz Poznámka 3.2). K jejímu nalezení zde použijeme způsob, jenž je možné nalézt ve článku [7]. Nejprve si tedy ukážeme platnost několika pomocných výroků:

Věta 4.2 *Nechť* $p_1 < p_2 < \cdots < p_i < \ldots$ *je posloupnost všech prvočísel ve tvaru* $p_i = 4k+3$, $k \in \mathbb{Z}_0^+$ *a* $D_i = \{m \cdot p_i^{2j} \mid j \in \mathbb{Z}_0^+,\ m \in \mathbb{N},\ \gcd(m, p_i) = 1\}$, *jinak řečeno* D_i *je množina všech přirozených čísel, která ve svém kanonickém rozkladu nemají prvočíslo* p_i *s lichou mocninou. Potom* $d(D_i) = \frac{p_i}{p_i+1}$.

Důkaz. Nejprve definujme množinu F_k jako množinu takových přirozených čísel, která mají v rozkladu prvočíslo p_i s mocninou větší nebo rovnou k. Odtud můžeme psát

$$\begin{aligned}
F_0 &= \mathbb{N} = \{m \mid m \in \mathbb{N}\} \quad \text{a} \quad F_0(n) = [n], \\
F_1 &= \{p_i \cdot m \mid m \in \mathbb{N}\} \quad \text{a} \quad F_1(n) = \left[\tfrac{n}{p_i}\right], \\
F_2 &= \{p_i^2 \cdot m \mid m \in \mathbb{N}\} \quad \text{a} \quad F_2(n) = \left[\tfrac{n}{p_i^2}\right], \\
&\vdots \\
F_k &= \{p_i^k \cdot m \mid m \in \mathbb{N}\} \quad \text{a} \quad F_k(n) = \left[\tfrac{n}{p_i^k}\right].
\end{aligned}$$

Nyní pro $k = 1, 2, \ldots$ definujeme množiny G_k a Q_k rekurentně následujícím předpisem:

$$\begin{aligned}
G_1 &= F_0 \\
Q_k &= \bigcup_{i=0}^{k-1} (F_{2i} - F_{2i+1}) \\
G_k &= Q_k \cup F_{2k-1}.
\end{aligned} \tag{4.1}$$

To znamená, že množina Q_k obsahuje všechna přirozená čísla, která mají ve svém kanonickém rozkladu prvočíslo p_i se sudou mocninou menší než $2k-1$, zatímco množina G_k obsahuje všechna přirozená čísla, kromě těch, která mají ve svém kanonickém rozkladu prvočíslo p_i s lichou mocninou menší než $2k-1$. Je zřejmé, že

1. V případě, že $k = 1$ platí

$$G_1 = F_0 = \mathbb{N} \supseteq D_i \supseteq Q_1 = F_0 - F_1,$$

z čehož pro všechna $n \in \mathbb{N}$ plyne

$$G_1(n) = [n] \geq D_i(n) \geq Q_1(n) = [n] - \left[\frac{n}{p_i}\right].$$

2. V případě, že $k = 2$ platí

$$G_2 = Q_1 \cup F_2 \supseteq D_i \supseteq Q_2 = G_2 - F_3,$$

z čehož pro všechna $n \in \mathbb{N}$ plyne

$$G_2(n) = [n] - \left[\frac{n}{p_i}\right] + \left[\frac{n}{p_i^2}\right] \geq D_i(n) \geq Q_2(n) = [n] - \left[\frac{n}{p_i}\right] + \left[\frac{n}{p_i^2}\right] - \left[\frac{n}{p_i^3}\right].$$

3. A konečně, pro každé $k, n \in \mathbb{N}$ platí

$$G_k \supseteq D_i \supseteq Q_k,$$
$$G_k(n) = \sum_{j=0}^{2(k-1)} (-1)^j \left[\frac{n}{p_i^j}\right] \geq D_i(n) \geq Q_k(n) = \sum_{j=0}^{2k-1} (-1)^j \left[\frac{n}{p_i^j}\right].$$

Proto také můžeme říci, že pro každé $k, n \in \mathbb{N}$ platí

$$\frac{\sum_{j=0}^{2(k-1)} (-1)^j \left[\frac{n}{p_i^j}\right]}{n} \geq \frac{D_i(n)}{n} \geq \frac{\sum_{j=0}^{2k-1} (-1)^j \left[\frac{n}{p_i^j}\right]}{n}.$$

Pro $n \to \infty$ dostáváme pro libovolné pevné $k \in \mathbb{N}$

$$\lim_{n\to\infty} \frac{\sum_{j=0}^{2(k-1)} (-1)^j \left[\frac{n}{p_i^j}\right]}{n} \geq \limsup_{n\to\infty} \frac{D_i(n)}{n} \geq \liminf_{n\to\infty} \frac{D_i(n)}{n} \geq \lim_{n\to\infty} \frac{\sum_{j=0}^{2k-1} (-1)^j \left[\frac{n}{p_i^j}\right]}{n},$$

a protože k je pevné,

$$\sum_{j=0}^{2(k-1)} (-1)^j \frac{1}{p_i^j} \geq \limsup_{n\to\infty} \frac{D_i(n)}{n} \geq \liminf_{n\to\infty} \frac{D_i(n)}{n} \geq \sum_{j=0}^{2k-1} (-1)^j \frac{1}{p_i^j}.$$

Nakonec, s $k \to \infty$ získáváme

$$\lim_{k\to\infty} \sum_{j=0}^{2(k-1)} (-1)^j \frac{1}{p_i^j} \geq \limsup_{n\to\infty} \frac{D_i(n)}{n} \geq \liminf_{n\to\infty} \frac{D_i(n)}{n} \geq \lim_{k\to\infty} \sum_{j=0}^{2k-1} (-1)^j \frac{1}{p_i^j}$$

$$\frac{p_i}{p_i+1} \geq \limsup_{n\to\infty} \frac{D_i(n)}{n} \geq \liminf_{n\to\infty} \frac{D_i(n)}{n} \geq \frac{p_i}{p_i+1}$$
$$\overline{d}(D_i) = \underline{d}(D_i) = d(D_i) = \frac{p_i}{p_i+1}.$$

■

Věta 4.3 *Nechť D_i jsou množiny, definované ve Větě 4.2. Pak pro každé $n \in \mathbb{N}$ platí, že $d(\cap_{i=1}^n D_i) = \prod_{i=1}^n d(D_i) = \prod_{i=1}^n \frac{p_i}{p_i+1}$.*

Důkaz. Provedeme indukcí. Pro $n = 1$ je důkaz triviální a pro $n = 2$ analogický jako u důkazu Věty 4.2: Uvědomíme-li si, že $D_1 \cap D_2 = \{p_1^{2j_1} p_2^{2j_2} \cdot m \mid j_1, j_2 \in \mathbb{Z}_0^+,\ m \in \mathbb{N},\ \gcd(m, p_1) = \gcd(m, p_2) = 1\}$, potom k tomu, abychom ukázali, že $d(D_1 \cap D_2) = \frac{p_1}{p_1+1} \cdot \frac{p_2}{p_2+1}$ musíme definovat množiny F_k následovně:

$$\begin{aligned}
F_0 &= D_2 = \{m \mid m \in D_2\} \quad \text{a tak} \quad F_0(n) = D_2(n), \\
F_1 &= \{p_1 \cdot m \mid m \in D_2\} \quad \text{a tak} \quad F_1(n) = D_2\left(\left[\tfrac{n}{p_1}\right]\right), \\
F_2 &= \{p_1^2 \cdot m \mid m \in D_2\} \quad \text{a tak} \quad F_2(n) = D_2\left(\left[\tfrac{n}{p_1^2}\right]\right), \\
&\vdots \\
F_k &= \{p_1^k \cdot m \mid m \in D_2\} \quad \text{a tak} \quad F_k(n) = D_2\left(\left[\tfrac{n}{p_1^k}\right]\right).
\end{aligned}$$

Množiny G_k a Q_k, $k = 1, 2, \ldots$ definujeme způsobem, popsaným ve vztahu (4.1), podobným postupem jako dříve pak získáme, že pro všechna $k, n \in \mathbb{N}$ platí

$$G_k \supseteq D_1 \cap D_2 \supseteq Q_k,$$

takže můžeme psát

$$G_k(n) = \sum_{j=0}^{2(k-1)} (-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right) \geq (D_1 \cap D_2)(n) \geq Q_k(n) = \sum_{j=0}^{2k-1} (-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right).$$

Odtud pro všechna $k, n \in \mathbb{N}$ platí

$$\frac{\sum_{j=0}^{2(k-1)} (-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right)}{n} \geq \frac{(D_1 \cap D_2)(n)}{n} \geq \frac{\sum_{j=0}^{2k-1} (-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right)}{n}.$$

Označíme-li $D^* = D_1 \cap D_2$, pak pro $n \to \infty$ dostáváme pro každé pevné $k \in \mathbb{N}$ následující

nerovnosti:

$$\lim_{n\to\infty}\frac{\sum_{j=0}^{2(k-1)}(-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right)}{n}\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq\lim_{n\to\infty}\frac{\sum_{j=0}^{2k-1}(-1)^j D_2\left(\left[\frac{n}{p_i^j}\right]\right)}{n}$$

$$\lim_{n\to\infty}\sum_{j=0}^{2(k-1)}\frac{(-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right)}{n}\frac{\left[\frac{n}{p_1^j}\right]}{\left[\frac{n}{p_1^j}\right]}\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq\lim_{n\to\infty}\sum_{j=0}^{2k-1}\frac{(-1)^j D_2\left(\left[\frac{n}{p_1^j}\right]\right)}{n}\frac{\left[\frac{n}{p_1^j}\right]}{\left[\frac{n}{p_1^j}\right]}$$

$$d(D_2)\sum_{j=0}^{2(k-1)}(-1)^j\frac{1}{p_1^j}\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq d(D_2)\sum_{j=0}^{2k-1}(-1)^j\frac{1}{p_1^j}.$$

S $k\to\infty$ vidíme, že:

$$\lim_{k\to\infty}d(D_2)\sum_{j=0}^{2(k-1)}(-1)^j\frac{1}{p_1^j}\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq\lim_{k\to\infty}d(D_2)\sum_{j=0}^{2k-1}(-1)^j\frac{1}{p_1^j}$$

$$d(D_2)\frac{p_1}{p_1+1}\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq d(D_2)\frac{p_1}{p_1+1}$$

$$d(D_2)d(D_1)\geq\bar{d}(D^*)\geq\underline{\mathrm{d}}(D^*)\geq d(D_2)d(D_1).$$

A tedy skutečně, $d(D_1\cap D_2)=d(D_1)\cdot d(D_2)=\frac{p_1}{p_1+1}\cdot\frac{p_2}{p_2+1}$.

Této myšlenky použijeme k provedení indukčního kroku. Označme $D^*=\cap_{i=1}^{r-1}D_i$. Indukčním předpokladem dostáváme $d(D^*)=\prod_{i=1}^{r-1}d(D_i)=\prod_{i=1}^{r-1}\frac{p_i}{p_i+1}$ a nyní ukážeme, že $d(D^*\cap D_r)=\prod_{i=1}^{r}d(D_i)=\prod_{i=1}^{r}\frac{p_i}{p_i+1}$. Opět definujeme množiny F_k jako

$$\begin{aligned}
F_0 &= D_2=\{m\mid m\in D^*\}\quad\text{a tak}\quad F_0(n)=D^*(n),\\
F_1 &= \{p_r\cdot m\mid m\in D^*\}\quad\text{a tak}\quad F_1(n)=D^*\left(\left[\tfrac{n}{p_r}\right]\right),\\
F_2 &= \{p_r^2\cdot m\mid m\in D^*\}\quad\text{a tak}\quad F_2(n)=D^*\left(\left[\tfrac{n}{p_r^2}\right]\right),\\
&\vdots\\
F_k &= \{p_r^k\cdot m\mid m\in D^*\}\quad\text{a tak}\quad F_k(n)=D^*\left(\left[\tfrac{n}{p_r^k}\right]\right),
\end{aligned}$$

množiny G_k a Q_k, $k=1,2,\ldots$ opět vztahem (4.1) a analogicky jako dříve zjistíme, že pro všechna $k,n\in\mathbb{N}$

$$\frac{\sum_{j=0}^{2(k-1)}(-1)^j D^*\left(\left[\frac{n}{p_r^j}\right]\right)}{n}\geq\frac{(D^*\cap D_r)(n)}{n}\geq\frac{\sum_{j=0}^{2k-1}(-1)^j D^*\left(\left[\frac{n}{p_r^j}\right]\right)}{n}.$$

Označíme-li nyní $D^{**} = D^* \cap D_r$, pak s $n \to \infty$ získáme pro libovolné pevné $k \in \mathbb{N}$

$$\lim_{n\to\infty} \frac{\sum_{j=0}^{2(k-1)} (-1)^j D^* \left(\left[\frac{n}{p_r^j} \right] \right)}{n} \geq \bar{d}(D^{**}) \geq \underline{\mathrm{d}}(D^{**}) \geq \lim_{n\to\infty} \frac{\sum_{j=0}^{2k-1} (-1)^j D^* \left(\left[\frac{n}{p_r^j} \right] \right)}{n},$$

$$\lim_{n\to\infty} \sum_{j=0}^{2(k-1)} \frac{(-1)^j D^* \left(\left[\frac{n}{p_r^j} \right] \right)}{n} \frac{\left[\frac{n}{p_r^j} \right]}{\left[\frac{n}{p_r^j} \right]} \geq \bar{d}(D^{**}) \geq \underline{\mathrm{d}}(D^{**}) \geq \lim_{n\to\infty} \sum_{j=0}^{2k-1} \frac{(-1)^j D^* \left(\left[\frac{n}{p_r^j} \right] \right)}{n} \frac{\left[\frac{n}{p_r^j} \right]}{\left[\frac{n}{p_r^j} \right]}.$$

Protože k je pevné, můžeme psát

$$d(D^*) \cdot \sum_{j=0}^{2(k-1)} (-1)^j \frac{1}{p_r^j} \geq \bar{d}(D^{**}) \geq \underline{\mathrm{d}}(D^{**}) \geq d(D^*) \cdot \sum_{j=0}^{2k-1} (-1)^j \frac{1}{p_r^j},$$

$$d(D^*)d(D_r) \geq \bar{d}(D^{**}) \geq \underline{\mathrm{d}}(D^{**}) \geq d(D^*)d(D_r).$$

Nakonec, z indukčního předpokladu máme

$$\left(\prod_{i=1}^{r-1} d(D_i) \right) d(D_r) \geq \bar{d}(D^{**}) \geq \underline{\mathrm{d}}(D^{**}) \geq \left(\prod_{i=1}^{r-1} d(D_i) \right) d(D_r),$$

$$\prod_{i=1}^{r} d(D_i) \geq \limsup_{n\to\infty} \frac{(\cap_{i=1}^{r} D_i)(n)}{n} \geq \liminf_{n\to\infty} \frac{(\cap_{i=1}^{r} D_i)(n)}{n} \geq \prod_{i=1}^{r} d(D_i)$$

$$d\left(\cap_{i=1}^{r} D_i\right) = \prod_{i=1}^{r} d(D_i).$$

■

Věta 4.4 *Uvažme posloupnost prvočísel p_i z Věty 4.2. Pak pro každé $n \in \mathbb{N}$ platí*

$$\prod_{i=1}^{n} \left(1 + \frac{1}{p_i} \right) \geq \sum_{i=1}^{n} \frac{1}{p_i}.$$

Důkaz. Uvědomme si, že při roznásobování členů v součinu bychom jistě mohli u $n-1$ závorek vzít jako činitel jedničku a u zbylé závorky $\frac{1}{p_i}$, $i \in \{1, \ldots, n\}$. Pokud toto provedeme pro každou závorku a všechny zbylé členy vzniklé dalším roznásobováním označíme jako $r \in \mathbb{R}^+$, dostáváme

$$\left(1 + \frac{1}{p_1} \right) \cdot \left(1 + \frac{1}{p_2} \right) \cdot \ldots \cdot \left(1 + \frac{1}{p_n} \right) = \sum_{i=1}^{n} \frac{1}{p_i} + r.$$

■

Poslední věcí, kterou budeme k důkazu věty o hodnotě asymptotické hustoty množiny B_2 potřebovat, je následující slavný poznatek teorie čísel, jenž uvedeme bez důkazu.

Věta 4.5 (Dirichletova) *Nechť pro čísla $a, b \in \mathbb{N}$ platí $\gcd(a,b) = 1$. Pak aritmetická posloupnost $\{ax+b\}_{x=0}^{\infty}$ obsahuje nekonečně mnoho prvočísel. Navíc, řada $\sum_{p \equiv b (\mathrm{mod}\ a)} \frac{1}{p}$, kde p jsou prvočísla, diverguje.*

Věta 4.6 *Nechť $B_2 = \{a^2 + b^2 \in \mathbb{N} | a, b \in \mathbb{Z}\}$. Pak $d(B_2)$ existuje a je rovna 0.*

Důkaz. Na základě Věty 3.4 víme, že množina B_2 neobsahuje čísla, jež mají ve svém kanonickém rozkladu prvočísla ve tvaru $p_i = 4\mathrm{k}{+}3$ s lichou mocninou. Je tak zřejmé, že platí $B_2 = \cap_{i=1}^{\infty} D_i$, kde $D_i = \{m \cdot p_i^{2j} \mid j \in \mathbb{Z}_0^+, m \in \mathbb{N}, \gcd(m, p_i) = 1\}$, tedy pro všechna $k \in \mathbb{N}$ platí $B_2 \subseteq (\cap_{i=1}^{k} D_i)$. To znamená, že pro všechna $k, n \in \mathbb{N}$ můžeme psát

$$B_2(n) = (\cap_{i=1}^{\infty} D_i)(n) \leq (\cap_{i=1}^{k} D_i)(n),$$
$$\frac{B_2(n)}{n} \leq \frac{(\cap_{i=1}^{k} D_i)(n)}{n}.$$

Použijeme-li nyní Větu 4.3, pak pro každé pevně zvolené k dostáváme

$$0 \leq \liminf_{n\to\infty} \frac{B_2(n)}{n} \leq \limsup_{n\to\infty} \frac{B_2(n)}{n} \leq \prod_{i=1}^{k} \frac{p_i}{p_i + 1}.$$

Platí

$$0 \leq \prod_{i=1}^{k} \frac{p_i}{p_i+1} = \prod_{i=1}^{k} \frac{1}{1+\frac{1}{p_i}} = \frac{1}{\prod_{i=1}^{k}(1+\frac{1}{p_i})} \overset{\text{Věta 4.4}}{\leq} \frac{1}{\sum_{i=1}^{k} \frac{1}{p_i}},$$

proto můžeme na základě Věty 4.5 říct, že $\lim_{k\to\infty} \prod_{i=1}^{k} \frac{p_i}{p_i+1} = 0$, z čehož již okamžitě plyne

$$0 \leq \liminf_{n\to\infty} \frac{B_2(n)}{n} \leq \limsup_{n\to\infty} \frac{B_2(n)}{n} \leq 0$$
$$\overline{d}(B_2) = \underline{d}(B_2) = d(B_2) = 0.$$

■

4.3 Asymptotická hustota spektra

Dříve uvedený důsledek Věty 3.7 nám nyní pomůže určit asymptotickou hustotu množiny B_3.

Věta 4.7 *Nechť $A = \{4^j(8k+7) \mid j, k \in \mathbb{Z}_0^+\}$. Potom $d(A) = \frac{1}{6}$.*

Důkaz. Množinu A lze přepsat jako $A = \{4^j(8k-1) \mid j \in \mathbb{Z}_0^+, k \in \mathbb{N}\}$. Abychom mohli bezpečně určit počet čísel v daném tvaru, bylo by dobré ukázat, že množiny $A_j = \{4^j(8k-1) \,|k \in \mathbb{N}\}$ jsou navzájem disjunktní. Sporem ukážeme, že tomu tak skutečně je. Předpokládejme, že existují

$j_1, j_2 \in \mathbb{Z}_0^+$, $j_1 \neq j_2$ a $k_1, k_2 \in \mathbb{N}$ taková, že

$$4^{j_1}(8k_1 - 1) = 4^{j_2}(8k_2 - 1).$$

Bez újmy na obecnosti lze předpoládat, že $j_1 > j_2$, a tak

$$\begin{aligned} 4^{j_1 - j_2}(8k_1 - 1) &= 8k_2 - 1 \\ 4(4^{j_1 - j_2 - 1}(8k_1 - 1) - 2k_2) &= -1. \end{aligned}$$

Z toho by plynulo, že $4 \mid -1$, což je zjevně spor a můžeme tedy tvrdit, že $4^{j_1}(8k_1 - 1) \neq 4^{j_2}(8k_2 - 1)$ pro $j_1 \neq j_2$.

K určení asymptotické hustoty obecně potřebujeme znát předpis pro $A(n)$, tedy počet prvků množiny A, nepřesahujících číslo n. Nechť j_n je nejvyšší takové celé číslo, pro které existuje $k \in \mathbb{N}$, splňující $4^{j_n}(8k - 1) \leq n$. Potom pro všechna $j \in \{0, 1, \ldots, j_n\}$ platí:

$$\begin{aligned} 4^j(8k - 1) &\leq n \\ 8k - 1 &\leq \tfrac{n}{4^j} \\ k &\leq \tfrac{1}{4^j}\tfrac{n}{8} + \tfrac{1}{8} \\ k &= \left[\tfrac{1}{4^j}\tfrac{n}{8} + \tfrac{1}{8}\right]. \end{aligned}$$

Odtud vidíme, že pro dané j může číslo k nabývat hodnot $1, 2, \ldots, \left[\frac{1}{4^j}\frac{n}{8} + \frac{1}{8}\right]$. Tedy

$$A_j(n) = \left[\frac{1}{4^j}\frac{n}{8} + \frac{1}{8}\right],$$

a protože $A = \cup_{j=0}^{\infty} A_j$ a množiny A_j jsou navzájem disjunktní, musí platit

$$A(n) = \sum_{j=0}^{j_n} \left[\frac{1}{4^j}\frac{n}{8} + \frac{1}{8}\right].$$

Po úpravě dostáváme výraz pro $\frac{A(n)}{n}$:

$$\frac{A(n)}{n} = \frac{1}{n}\sum_{j=0}^{j_n}\left(\frac{1}{4^j}\frac{n}{8} + \frac{1}{8} - \varepsilon_j\right) = \underbrace{\frac{1}{8}\sum_{j=0}^{j_n}\frac{1}{4^j}}_{A_n} + \underbrace{\frac{1}{n}\sum_{j=0}^{j_n}\frac{1}{8}}_{B_n} - \underbrace{\frac{1}{n}\sum_{j=0}^{j_n}\varepsilon_j}_{C_n}, \tag{4.2}$$

kde $0 \leq \varepsilon_j < 1$.

Pro vyčíslení těchto výrazů, respektive příslušných limit, potřebujeme ještě znát hodnotu j_n v závislosti na n. Podle toho, jak jsme definovali číslo j_n víme, že výraz $4^{j_n+1}(8k - 1) > n$ pro

libovolné k a zároveň určitě existuje $k \in \mathbb{N}$, pro které platí $4^{j_n}(8k-1) \leq n$. Proto

$$\begin{array}{rcccl} 4^{j_n}(8\cdot 1-1) & \leq & n & < & 4^{j_n+1}(8\cdot 1-1) \\ \ln\left(7\cdot 4^{j_n}\right) & \leq & \ln n & < & \ln\left(7\cdot 4^{j_n+1}\right) \\ j_n \ln 4 + \ln 7 & \leq & \ln n & < & (j_n+1)\ln 4 + \ln 7 \\ j_n & \leq & \frac{\ln n - \ln 7}{\ln 4} & < & j_n + 1 \end{array}$$

a zjišťujeme tak, že $j_n = \left[\frac{\ln n - \ln 7}{\ln 4}\right]$. Samotnou asymptotickou hustotu vypočteme následovně:

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n} = \lim_{n\to\infty} A_n + \lim_{n\to\infty} B_n - \lim_{n\to\infty} C_n. \tag{4.3}$$

Stačí nám spočítat jednotlivé dílčí limity, začneme s limitou C_n. Platí

$$\begin{array}{rcccl} 0 & \leq & \frac{1}{n}\sum_{j=0}^{j_n} \varepsilon_j & < & \frac{1}{n}\sum_{j=0}^{j_n} 1 \\ 0 & \leq & C_n & < & \frac{1}{n}(j_n+1) \\ 0 & \leq & C_n & < & \frac{1}{n}\left(\left[\frac{\ln n - \ln 7}{\ln 4}\right]+1\right). \end{array} \tag{4.4}$$

Posloupnost n roste výrazně rychleji, nežli $\ln n$, a tedy i prostou úvahou vidíme, že $\lim_{n\to\infty} \frac{1}{n}\left(\left[\frac{\ln n - \ln 7}{\ln 4}\right]+1\right) = 0$ (o čemž se lze snadno přesvědčit aplikací l'Hospitalova pravidla), čili ze vztahu (4.4) plyne, že

$$\lim_{n\to\infty} C_n = \lim_{n\to\infty} \frac{1}{n}\sum_{j=0}^{j_n} \varepsilon_j = 0. \tag{4.5}$$

Obdobná situace nastane pro B_n:

$$\lim_{n\to\infty} B_n = \lim_{n\to\infty} \frac{1}{n}\sum_{j=0}^{j_n} \frac{1}{8} = \lim_{n\to\infty} \frac{1}{8n}\left(\left[\frac{\ln n - \ln 7}{\ln 4}\right]+1\right) = 0. \tag{4.6}$$

Zbývá vyřešit limitu pro A_n. Všimněme si, že $\sum_{j=0}^{j_n} \frac{1}{4^j}$ je součet prvních j_n+1 členů geometrické posloupnosti, kde $a_0 = 1$ a $q = \frac{1}{4}$. Díky tomu vidíme, že

$$\begin{aligned}
\lim_{n\to\infty} A_n &= \lim_{n\to\infty} \tfrac{1}{8} \textstyle\sum_{j=0}^{j_n} \frac{1}{4^j} \\
&= \lim_{n\to\infty} \tfrac{1}{8} \frac{1-\left(\frac{1}{4}\right)^{j_n+1}}{1-\frac{1}{4}} \\
&= \tfrac{1}{8} \cdot \lim_{n\to\infty} \frac{1-\left(\frac{1}{4}\right)^{\left[\frac{\ln n - \ln 7}{\ln 4}\right]+1}}{1-\frac{1}{4}} \\
&= \tfrac{1}{8} \cdot \tfrac{1}{\frac{3}{4}} \\
&= \tfrac{1}{6}.
\end{aligned} \tag{4.7}$$

Nakonec spojením předpisu (4.3) a mezivýsledků (4.5), (4.6) a (4.7) pak dostáváme, že $d(A) = \frac{1}{6}$. ∎

Nyní už na základě Věty 4.7, důsledku Věty 3.7 a 5. bodu Věty 4.1 vidíme, že pro asymptotickou hustotu množiny B_3 platí

$$d(B_3) = d(\mathbb{N}) - d(A) = 1 - \frac{1}{6} = \frac{5}{6}. \tag{4.8}$$

Věta 4.8 *Nechť S_E označuje energetické spektrum částice v trojrozměrné pravoúhlé potenciálové jámě nekonečné hloubky. Pak $d(S_E) = \frac{5}{6}$.*

Důkaz. Zjevně platí $B_3 \supseteq S_E \supseteq (B_3 - B_2)$. Odtud

$$\begin{array}{rcccccl}
B_3(n) & \geq & S_E(n) & \geq & (B_3 - B_2)(n) & \geq & B_3(n) - B_2(n) \\
\lim\limits_{n\to\infty} \frac{B_3(n)}{n} & \geq & \limsup\limits_{n\to\infty} \frac{S_E(n)}{n} & \geq & \liminf\limits_{n\to\infty} \frac{S_E(n)}{n} & \geq & \lim\limits_{n\to\infty} \frac{B_3(n)}{n} - \lim\limits_{n\to\infty} \frac{B_2(n)}{n} \\
d(B_3) & \geq & \overline{d}(S_E) & \geq & \underline{d}(S_E) & \geq & d(B_3) - d(B_2) \\
\frac{5}{6} & \geq & \overline{d}(S_E) & \geq & \underline{d}(S_E) & \geq & \frac{5}{6} - 0
\end{array}$$

$$d(S_E) = \frac{5}{6}.$$

∎

Poznámka 4.1 Pro stručnost budeme množinu přípustných energetických hladin částice v nekonečně hluboké pravoúhlé potenciálové jámě i nadále značit S_E.

5 Testování počtu částic v potenciálové jámě

V této kapitole se čistě teoreticky zamyslíme, jak bychom na základě měření energie systému určili, zda se v jámě nachází právě jedna či více částic. Nejprve si však připomeneme princip testování hypotéz.

5.1 Testování statistických hypotéz

Jedná se o rozhodovací proces, při němž se snažíme na základě naměřených hodnot ověřit pravdivost nějakého výroku, který se obecně označuje jako **nulová hypotéza** a značí se H_0. Postup při rozhodování je pak následovný:

1. Samotné stanovení H_0,
2. volba testové statistiky, tj. nalezení náhodné veličiny T, jejíž rozdělení známe, za předpokladu, že platí H_0,
3. určení, nakolik „pravděpodobné“ hodnoty náhodné veličiny T jsme naměřili. Míru této pravděpodobnosti vyjadřuje tzv. **p-hodnota**. Čím více se tato hodnota blíží nule, tím více to vypovídá v neprospěch platnosti H_0.

Poznámka 5.1 V praxi se většinou v protikladu k H_0 staví **alternativní hypotéza** H_A, jejíž tvrzení je nějakým způsobem v rozporu s H_0, často formulováno podle toho, nač ukazují data (např. když chceme otestovat, zda je střední hodnota rovna 0, položíme $H_0 : \ \mu = 0$, nicméně průměr naměřených hodnot je 4, a tak klademe $H_A : \ \mu > 0$).

Pokud konstruujeme test tak, že se snažíme H_0 na základě naměřených dat zamítnout, tak jako to později uděláme i zde, můžeme tento zjednodušený postup testování hypotéz označit za jakousi statistickou analogii matematického důkazu sporem.

Nabízí se otázka, podle čeho rozhodnout, kdy se přikloníme k zamítnutí H_0 a kdy ji ještě ponecháme jakožto pravděpodobnou variantu. K tomu slouží tzv. **hladina významnosti**. Jedná se o jakousi spolehlivost testu, již si předem určíme. Konkrétně jde o pravděpodobnost, že zamítneme H_0, ačkoliv ve skutečnosti je její tvrzení platné. V souvislosti s tím pak můžeme p-hodnotu definovat také jako nejnižší hladinu významnosti, na níž lze H_0 zamítnout.

5.2 Test hypotézy o počtu částic

Víme již, že jedna částice sama o sobě má, při vhodné volbě jednotek, energii E rovnu součtu tří druhých mocnin přirozených čísel, viz předpis (2.22). Můžeme tak říct, že $E \in S_E$. Pokud se v jámě nachází $k \geq 2$ částic, pak je celková energie (neuvažujeme-li vzájemné interakce částic) daná součtem $3k$ druhých mocnin. Díky Lagrangeově větě (Věta 3.8) však víme, že každé přirozené číslo lze vyjádřit jako součet čtyř druhých mocnin celých čísel. Z toho můžeme

usuzovat, že pokud se v jámě nachází více než jedna částice, může celková energie částic v ní uvězněných nabývat teoreticky libovolné hodnoty z $\mathbb{N}$.

Představme si tedy, že jsme schopni energii soustavy v potenciálové jámě měnit a opakovaně měřit. Pokusme se určit pravděpodobnost, že obecně v prvních n měřeních bude naměřená energie pokaždé součtem tří druhých mocnin celých čísel. Předpokládejme, že jednotlivá měření jsou na sobě nezávislá, zároveň že u každého z nich máme teoreticky stejnou pravděpodobnost, že dostaneme číslo vyjádřitelné jako součet tří čtverců. Konkrétně na základě vztahu (4.8) je tato pravděpodobnost rovna $\frac{5}{6}$.

Poznámka 5.2 Zda je hodnota energie součtem tří čtverců můžeme ověřit algoritmicky, viz Kapitola 6, případně Příloha A.

Pokud si jako náhodnou veličinu X zvolíme počet pokusů do prvního naměření hodnoty mimo množinu S_E, pak se X řídí **geometrickým rozdělením** pravděpodobnosti. Fakt, že náhodná veličina má geometrické rozdělení pravděpodobnosti zapisujeme $X \sim Ge(p)$, kde p je pravděpodobnost úspěchu. Náhodná veličina s geometrickým rozdělením totiž popisuje právě počet pokusů do prvního úspěchu včetně. V našem případě je parametrem p pravděpodobnost, že výsledek měření padne mimo množinu S_E, takže $p = \frac{1}{6}$.

Pravděpodobnost, že náhodná veličina X nabude hodnoty $n \in \mathbb{N}$ má předpis

$$P(X = n) = p(1-p)^{n-1}. \tag{5.1}$$

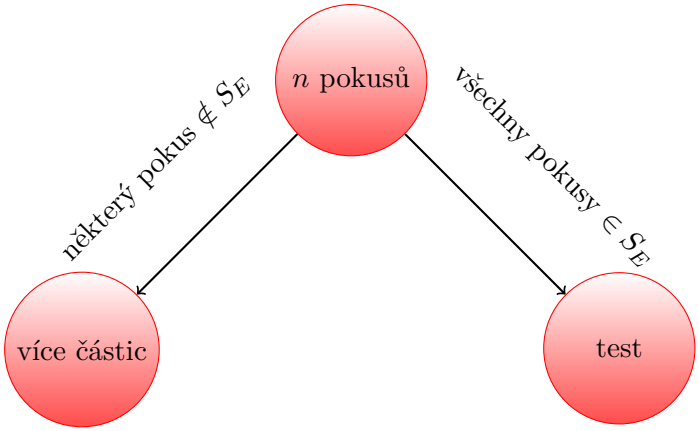
Budeme-li pravděpodobnost, že v každém z $n-1$ pokusů vyjde součet tří čtverců, a teprve v n-tém pokuse ne, tabelovat pro různá n, dostaneme následující tabulku:

n	$P(X = n)$
1	0.16666
5	0.08038
10	0.03230
20	0.00521
50	0.00002
100	$2.01 \cdot 10^{-9}$

Tabulka 2: Vybrané hodnoty pravděpodobnostní funkce náhodné veličiny X

Na základě Tabulky 2 je jasně vidět, že pravděpodobnost se zvyšujícím se n prudce klesá.

Pokud bychom nyní chtěli na základě měření určit, zda je v jámě jedna či více částic, musíme si uvědomit následující - jakmile naměříme hodnotu, která nespadá do množiny S_E, pak víme, že v jámě je více než jedna částice. V opačném případě, tj. pokud v prvních n měřeních pokaždé naměříme energii, která by tvarem odpovídala jedné částici, můžeme formulovat test o počtu částic.



Obrázek 1: Rozhodovací proces pro počet částic

Pokusme se zkonstruovat test, který by nám dal odpověď na otázku, zda je v potenciálové jámě částic více, než jedna, v případě, že jsme v n měřeních za sebou naměřili hodnotu z množiny S_E. Počet částic označme k. Jak jsme viděli výše, s rostoucím n se pravděpodobnost, že naměřená energie bude pokaždé z množiny S_E razantně snižuje. Proto položme
$H_0: \ k > 1$
$H_A: \ k = 1.$
Nyní potřebujeme vhodně zvolit testovou statistiku $T(X)$. Pro naše účely bude výhodné zavést $T(X) = n$, tedy počet po sobě jdoucích měření, jež všechna byla prvky množiny S_E. Na základě toho můžeme říct, že nulové rozdělení se shoduje s geometrickou náhodnou veličinou. To však neznamená nic jiného, než že pro p-hodnotu (pro stručnost ji označme p_h) platí

$$\begin{aligned} p_h &= P(X > n) = 1 - F(n+1) = 1 - \sum_{i=1}^{n} \tfrac{1}{6} \cdot \left(\tfrac{5}{6}\right)^{i-1} \\ &= 1 - \tfrac{1}{6} \cdot \tfrac{1-\left(\frac{5}{6}\right)^n}{1-\frac{5}{6}} = 1 - \left(1 - \left(\tfrac{5}{6}\right)^n\right) = \left(\tfrac{5}{6}\right)^n. \end{aligned} \tag{5.2}$$

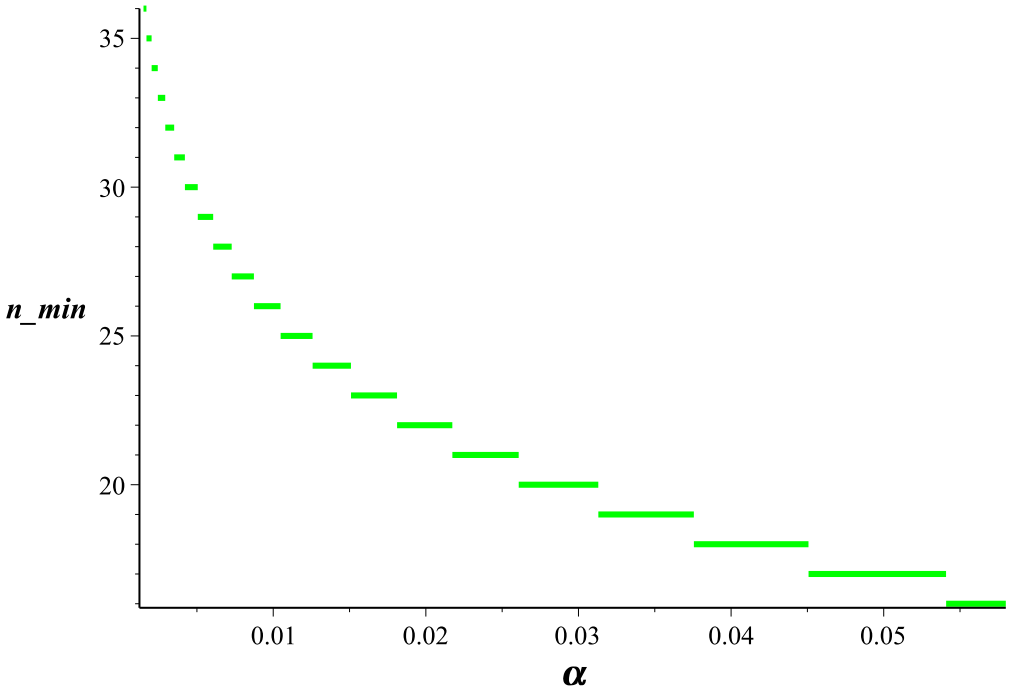
Zda můžeme H_0 zamítnout očividně závisí na čísle n a také samozřejmě na zadané hladině významnosti α. Zřejmě platí, že pokud je p-hodnota nižší, než α, můžeme zamítnout H_0 ve prospěch H_A.

Tento přístup by byl velmi výhodný v tom, že bychom mohli celý proces v zásadě otočit. Nejprve bychom si stanovili, s jakou mírou spolehlivosti chceme počet částic otestovat (tj. jaké zvolíme α). Na základě předpisu p-hodnoty je pak možné spočítat, kolikrát za sebou bychom

museli naměřit energii z množiny S_E:

$$\begin{aligned} p_h &< \alpha \\ \left(\tfrac{5}{6}\right)^n &< \alpha \\ n &> \log_{\frac{5}{6}} \alpha \\ n &> \tfrac{\ln \alpha}{\ln \frac{5}{6}}. \end{aligned} \tag{5.3}$$

Výpočet (5.3) nám ukazuje, že minimální počet pokusů, v nichž musí vyjít energie z množiny S_E, aby bylo možno zamítnout H_0 na zadané hladině významnosti, je $n_{min} = \left[\frac{\ln \alpha}{\ln \frac{5}{6}}\right] + 1$.



Obrázek 2: Graf závislosti n_{min} na hladině významnosti

Příjemným faktem je, že by při našem pokusu nebylo zapotřebí tisíců měření, neboť pro nejběžněji užívané hladiny významnosti 0.05 a 0.01 je hodnota n_{min} rovna 17, respektive 26.

5.3 Bayesovský přístup

V závislosti na počtu měření jsme tedy byli při zvolené hladině významnosti schopni testovat, zda se v jámě nachází právě jedna částice. Podívejme se teď na celý problém v jiném světle. Použijeme Bayesovský přístup. Ten je založený na podmíněných pravděpodobnostech, proto si nejprve uveďme nezbytné pojmy:

Definice 5.1 *Nechť (Ω, S, P) je pravděpodobnostní prostor, $A, B \in S$ jsou náhodné jevy a $P(B) > 0$. Pak* ***podmíněnou pravděpodobnost*** *jevu A za podmínky B definujeme vztahem*

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}.$$

Obdobně se dá pro náhodný vektor (X, Y) definovat podmíněná hustota pravděpodobnosti vztahem

$$f(x|y) = \frac{f(x, y)}{f(y)}.$$

Poznámka 5.3 Pomocí podmíněné pravděpodobnosti se často počítá pravděpodobnost průniku jevů jako $P(A \cap B) = P(A \mid B) \cdot P(B) = P(B \mid A) \cdot P(A)$. Za předpokladu, že jsou příslušné podmíněné pravděpodobnosti definovány, lze toto pravidlo pomocí „zřetězení“ zobecnit na průnik libovolného konečného počtu jevů:

$$P\left(\bigcap_{i=1}^{n} A_i\right) = \prod_{j=1}^{n} P\left(A_j \mid \bigcap_{k=1}^{j-1} A_k\right). \tag{5.4}$$

Věta 5.1 (Bayesova) *Nechť (X, Y) je náhodný vektor. Potom platí*

$$f(y|x) = \frac{f(x|y) \cdot f(y)}{f(x)}.$$

Definice 5.2 *Nechť (Ω, S, P) je pravděpodobnostní prostor, $A, B, C \in S$. Jevy A a B nazveme* ***podmíněně nezávislé*** *za podmínky, že nastal jev C, právě tehdy, když*

$$P(A \cap B \mid C) = P(A \mid C) \cdot P(B \mid C).$$

Poznámka 5.4 Podmíněně nezávislé jevy tedy můžeme interpretovat tak, že pokud nastal náhodný jev C, pak nám výskyt náhodného jevu A nedává žádnou informaci o pravděpodobnosti výskytu náhodného jevu B a naopak. Z předchozí definice opět můžeme odvodit vztah pro náhodné jevy A, B podmíněně nezávislé za podmínky C, jenž později použijeme při úpravách:

$$P(A \mid B \cap C) = \frac{P(A \cap B \cap C)}{P(B \cap C)} = \frac{P(A \cap B \mid C) \cdot P(C)}{P(B \mid C) \cdot P(C)} = P(A \mid C). \tag{5.5}$$

Nyní ve stručnosti nastiňme princip Bayesovského odhadu. Základní myšlenkou je, že na neznámý parametr nenahlížíme jako na konstantu, nýbrž jako na náhodnou veličinu. Zatímco běžně značíme hustotu náhodné veličiny X s nějakým parametrem θ pouze jako $f(x)$, v Bayesovském přístupu, kde je θ hodnotou náhodné veličiny, musíme psát $f(x \mid \theta)$. Pro náhodnou veličinu popisující parametr θ pak zavádíme hustotu pravděpodobnosti $f(\theta)$, tzv. **apriorní hustotu**. Tu volíme tak, abychom do ní zakomponovali informace, které o neznámém parametru máme, ať

už se jedná o výsledky měření, či obecné vlastnosti daného parametru. Na základě této hustoty potom odvozujeme **aposteriorní hustotu** $f(\theta \mid x) \propto f(x \mid \theta) \cdot f(\theta)$, kde konstantou úměrnosti je $\frac{1}{f(x)}$. Hodnotu $f(x)$ můžeme získat ze sdružené hustoty pravděpodobnosti $f(x, \theta)$ integrací:

$$f(x) = \int f(x, \theta) \mathrm{d}\theta = \int f(x \mid \theta) \cdot f(\theta) \mathrm{d}\theta,$$

přičemž uvedenou integraci chápeme jako určitý integrál přes celý obor hodnot veličiny Θ.

Představme si tedy, že máme t krabic a u každé provádíme nejvýše n měření. Pro i-tý systém definujme následující náhodné veličiny:

$$\begin{aligned} H_i &= \begin{cases} 0 \Leftrightarrow k_i > 1 \\ 1 \Leftrightarrow k_i = 1 \end{cases} \\ T_i &= \begin{cases} 0 \Leftrightarrow \exists j \in \{1, 2, \ldots, n\} : E_{i,j} \notin S_E \\ 1 \Leftrightarrow \forall j \in \{1, 2, \ldots, n\} : E_{i,j} \in S_E \end{cases} . \end{aligned} \tag{5.6}$$

Poznámka 5.5 Ačkoliv náhodné veličiny H_i, T_i jsou zjevně diskrétní, použijeme hustotu pravděpodobnosti. Tento přístup je korektní, pokud se na pravděpodobnostní funkci díváme jako na hustotu pravděpodobnosti vzhledem k čítací míře[4], namísto Lebesgueovy míry.

Chování náhodné veličiny H_i, vzhledem k jejímu zavedení, zatím nemůžeme nijak predikovat, neboť na pravděpodobnost H_i za podmínky t provedených měření se ptáme. Můžeme se však podívat na pravděpodobnost T_i v souvislosti se skutečným stavem. Označme Θ náhodnou veličinu popisující pravděpodobnost, že se v jámě nachází právě jedna částice:

$$f(T_i | H_i = 0) = \begin{cases} 1 - \left(\frac{5}{6}\right)^n \Leftrightarrow T_i = 0 \\ \left(\frac{5}{6}\right)^n \Leftrightarrow T_i = 1 \end{cases} \tag{5.7}$$

$$f(T_i | H_i = 1) = \begin{cases} 0 \Leftrightarrow T_i = 0 \\ 1 \Leftrightarrow T_i = 1 \end{cases} \tag{5.8}$$

[4]Čítaci míra je zobrazení μ, které množině A přiřadí číslo $\mu(A)$ předpisem

$$\mu(A) = \begin{cases} |A| & \Leftrightarrow A \text{ je konečná} \\ \infty & \Leftrightarrow A \text{ je nekonečná} \end{cases}$$

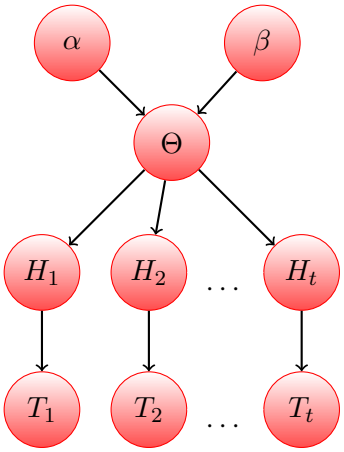
$$f(H_i|\theta) \quad = \quad \begin{cases} 1-\theta \;\Leftrightarrow\; H_i = 0 \\ \theta \;\Leftrightarrow\; H_i = 1 \end{cases} . \tag{5.9}$$

Parametr $\theta \in \langle 0, 1\rangle$ představuje konkrétní hodnotu veličiny Θ. Nyní zvolíme apriorní rozdělení parametru.

U modelu (5.9), který jsme zavedli[5], se z praktických důvodů ukazuje výhodným použít pro apriorní odhad **Beta rozdělení**. Dá se totiž ukázat, že pro tento model zůstává i aposteriorní hustota daná Beta rozdělením. Toto rozdělení má 2 parametry α a β, zapisujeme $\Theta \sim \text{Beta}(\alpha, \beta)$, a hustotu pravděpodobnosti

$$f(\theta) = \frac{1}{B(\alpha,\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1}, \tag{5.10}$$

přičemž $B(\alpha,\beta) = \int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\mathrm{d}x$ je Beta funkce, která v tomto případě plní roli normovací konstanty.



Obrázek 3: Grafový model pro zavedené náhodné veličiny

Poznámka 5.6 Naše situace je o něco složitější, neboť (jak je také patrné z obrázku 3) nepozorujeme hodnoty veličin H_i přímo, nýbrž prostřednictvím jednotlivých měření T_i. Z grafu také mimo jiné plyne, že veličiny T_i, Θ jsou podmíněně nezávislé za podmínky H_i.

Podívejme se teď na pravděpodobnost T_i za podmínky $\Theta = \theta$:

$$f(T_i|\theta) = \sum_{H_i\in\{0,1\}} f(T_i, H_i|\theta) = \sum_{H_i\in\{0,1\}} f(T_i|H_i)\cdot f(H_i|\theta)$$

$$f(T_i|\theta) = \begin{cases} \left(1-\left(\frac{5}{6}\right)^n\right)\cdot(1-\theta) \;\Leftrightarrow\; T_i = 0 \\ \left(\frac{5}{6}\right)^n\cdot(1-\theta)+\theta \;\Leftrightarrow\; T_i = 1 \end{cases} . \tag{5.11}$$

[5]Tento model se označuje jako **Beta-binomial model**.

Z apriorní hustoty a zavedeného modelu určíme aposteriorní hustotu parametru θ. Označme $T_{1:t} = (T_1, T_2, \ldots, T_t)$. S užitím Bayesovy věty potom platí

$$\begin{aligned} f(\theta|T_{1:t}) &\propto f(T_{1:t}|\theta) \cdot f(\theta) = f(\theta) \cdot \prod_{i=1}^{t} f(T_i|\theta) = \\ &= f(\theta) \cdot \left[\left(1 - \left(\frac{5}{6}\right)^n\right) \cdot (1-\theta)\right]^{t-V} \cdot \left[\left(\frac{5}{6}\right)^n \cdot (1-\theta) + \theta\right]^{V} \propto \\ &\propto f(\theta) \cdot (1-\theta)^{t-V} \cdot \left[\left(\frac{5}{6}\right)^n \cdot (1-\theta) + \theta\right]^{V}, \end{aligned} \tag{5.12}$$

s tím, že $V = \sum_{i=1}^{t} T_i$, tedy počet všech $T_i = 1$. Samotnou aposteriorní hustotu pravděpodobnosti parametru θ za předpokladu t pokusů, pak vypočteme normováním jako

$$f(\theta|T_{1:t}) = \frac{f(\theta) \cdot (1-\theta)^{t-V} \cdot \left[\left(\frac{5}{6}\right)^n \cdot (1-\theta) + \theta\right]^{V}}{\int_0^1 f(\theta^*) \cdot (1-\theta^*)^{t-V} \cdot \left[\left(\frac{5}{6}\right)^n \cdot (1-\theta^*) + \theta^*\right]^{V} \mathrm{d}\theta^*}. \tag{5.13}$$

Poznámka 5.7 Jelikož $\left(1 - \left(\frac{5}{6}\right)^n\right)$ je při daném n konstanta nezávislá na θ, mohli jsme ji zahrnout do přímé úměry, a proto vynechat z výrazu (5.12). Nelze to však provést i se zbylým $\left(\frac{5}{6}\right)^n$, protože celý výraz, umocněný na V, je součtem. Toto nepříjemné ztížení je dáno dříve zmíněným faktem, že nepozorujeme přímo hodnoty veličin H_i. Pokud bychom H_i pozorovali, zůstalo by nám pouze θ^V. Všimněme si, že potom by výsledkem skutečně bylo Beta rozdělení s parametry $(\alpha + V)$ a $(\beta + t - V)$.

Nakonec se pokusíme určit pravděpodobnost, že při $(t+1)$-ním pokusu bude hodnota H_{t+1} rovna 0, resp. 1, na základě pozorovaných hodnot $T_1, \ldots, T_{t+1}$:

$$f(H_{t+1}|T_{1:t}, T_{t+1}) = \frac{f(H_{t+1}, T_{1:t}|T_{t+1})}{f(T_{t+1}|T_{1:t})} = \frac{f(H_{t+1}, T_{1:t}|T_{t+1})}{\sum\limits_{H_{t+1} \in \{0,1\}} f(H_{t+1}, T_{1:t}|T_{t+1})}$$

$$\begin{aligned} f(H_{t+1}, T_{1:t}|T_{t+1}) &= \int_0^1 f(H_{t+1}, T_{1:t}, \theta|T_{t+1})\mathrm{d}\theta = \\ &= \int_0^1 f(T_{t+1}|H_{t+1}, T_{1:t}, \theta) \cdot f(H_{t+1}|T_{1:t}, \theta) \cdot f(\theta|T_{1:t})\mathrm{d}\theta = \\ &= \int_0^1 f(T_{t+1}|H_{t+1}) \cdot f(H_{t+1}|\theta) \cdot f(\theta|T_{1:t})\mathrm{d}\theta. \end{aligned}$$

Odtud

$$f(H_{t+1}|T_{1:t}, T_{t+1} = 0) = \begin{cases} 0 \;\Leftrightarrow\; H_{t+1} = 1 \\ 1 \;\Leftrightarrow\; H_{t+1} = 0 \end{cases} \tag{5.14}$$

$$f(H_{t+1}|T_{1:t}, T_{t+1}=1) = \begin{cases} \dfrac{\int_0^1 \theta\cdot f(\theta|T_{1:t})\mathrm{d}\theta}{\left(\frac{5}{6}\right)^n \int_0^1 (1-\theta)\cdot f(\theta|T_{1:t})\mathrm{d}\theta + \int_0^1 \theta\cdot f(\theta|T_{1:t})\mathrm{d}\theta} & \Leftrightarrow \ H_{t+1}=1 \\ \\ \dfrac{\left(\frac{5}{6}\right)^n \int_0^1 (1-\theta)\cdot f(\theta|T_{1:t})\mathrm{d}\theta}{\left(\frac{5}{6}\right)^n \int_0^1 (1-\theta)\cdot f(\theta|T_{1:t})\mathrm{d}\theta + \int_0^1 \theta\cdot f(\theta|T_{1:t})\mathrm{d}\theta} & \Leftrightarrow \ H_{t+1}=0 \end{cases} . \tag{5.15}$$

Uvedený model tedy využívá aposteriorní hustotu, a předchozích t měření k tomu, abychom na základě výsledku $(t+1)$-ního měření mohli odhadnout pravděpodobnost pro hodnotu veličiny H_{t+1}.

Nyní si můžeme pomoci simulací a zavedený model vyzkoušet. Na okamžik zapomeneme, že skutečnou hodnotu parametru θ neznáme a nějak si ji zvolíme. Na základě zvolené hodnoty a definic náhodných veličin H_i a T_i si pak domnělá měření T_i můžeme při daném n a t nechat náhodně vygenerovat a na ně aplikovat získané poznatky.

Příklad 5

Zvolme si nyní $\theta = \frac{1}{4},\ t = n = 20$. Postupujeme následovně:

1. Nejprve si vygenerujeme vektor H tak, že $H_i = 1$ s pravděpodobností θ. Může nám vyjít například takovýto vektor:

$$H = (0,1,0,0,1,0,1,0,0,0,0,0,1,0,0,0,1,0,0,0)\,.$$

2. Dále vektoru T přisoudíme 1 na těch pozicích, kde je má i H. Ostatní pozice vektoru T zaplníme tak, že pro každou z těchto pozic vygenerujeme 20 pokusů s výsledkem úspěch/neúspěch a pravděpodobností úspěchu $\frac{5}{6}$. Pouze tam, kde se dvacetkrát nageneroval úspěch přisoudíme na danou pozici ve vektoru T další jedničku.

$$T = (0,1,0,0,1,0,1,0,0,0,0,1,1,0,0,0,1,0,0,0)\,.$$

   Vidíme, že vyšla jedna jednička navíc, konkrétně na 12. pozici.

3. Jediná informace, kterou o nyní již hledaném parametru θ máme je ta, že se jedná o pravděpodobnost, tedy číslo z intervalu $\langle 0,1\rangle$. Abychom nezanesli do modelu přebytečnou informaci, zvolíme jako apriorní rozdělení Beta $\left(\frac{1}{2},\frac{1}{2}\right)$. Toto rozdělení je také známé jako **Jeffreysovo neinformativní rozdělení**, viz [14].

4. Spočítáme hodnotu V, v našem případě tedy $V = 6$.

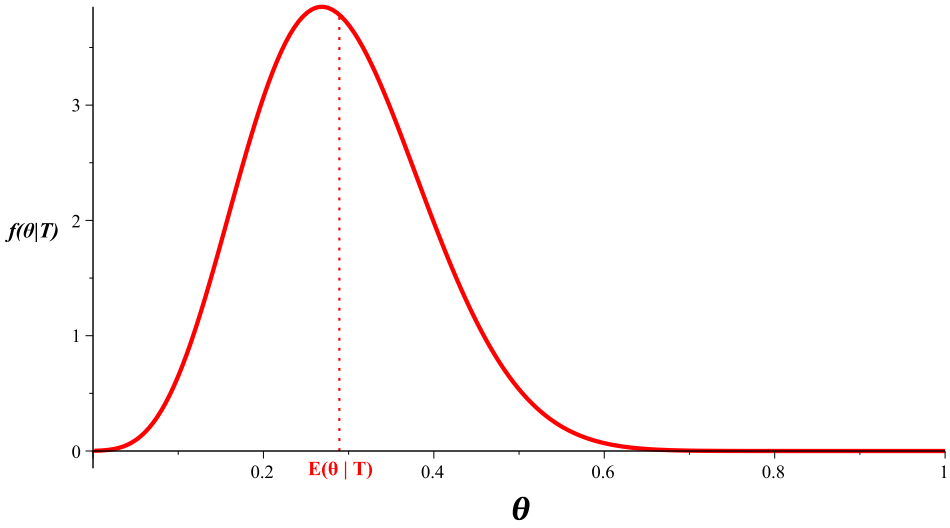
5. Tím máme vše potřebné pro předpis aposteriorní hustoty:

$$f(\theta|T_{1:20}) = \frac{(1-\theta)^{14} \cdot \left[\left(\frac{5}{6}\right)^{20} \cdot (1-\theta) + \theta\right]^6}{\pi\sqrt{\theta} \cdot \sqrt{1-\theta} \int_0^1 f(\theta^*) \cdot (1-\theta^*)^{14} \cdot \left[\left(\frac{5}{6}\right)^{20} \cdot (1-\theta^*) + \theta^*\right]^6 \mathrm{d}\theta^*}.$$

Než přikročíme k výpočtu samotné pravděpodobnosti, nabízí se otázka, jaká je asi střední hodnota této aposteriorní hustoty. Na tu můžeme použít známý vztah

$$E(\theta|T_{1:20}) = \int_0^1 \theta \cdot f(\theta|T_{1:20})\mathrm{d}\theta,$$

ale již integrál určující samotnou aposteriorní hustotu není analyticky řešitelný, tedy není řešitelný ani integrál při hledání střední hodnoty. Nezbývá nám, než nasadit výpočetní techniku a numerické metody. Výsledkem je hodnota $E(\theta|T_{1:20}) = 0,2891$, což je skutečně poměrně blízko námi „stanovené“ hodnotě $\theta = \frac{1}{4}$. Pro ilustraci můžeme uvést graf aposteriorní hustoty:



Obrázek 4: Graf aposteriorní hustoty $f(\theta|T_{1:20})$ pro naši simulaci

6. Nakonec předpokládejme, že jsme při 21. pokusu naměřili v jámě opět dvacetkrát za sebou hodnotu z množiny S_E. Dosazením do vztahu (5.15) a počítačovým výpočtem pak dostáváme

$$f(H_{21} = 1|T_{1:20}, T_{21} = 1) = 0,9397.$$

■

6 Algoritmus rozkladu čísla na součet tří čtverců

V této stručné kapitole se zběžně podíváme na algoritmický rozklad přirozeného čísla na součet tří celočíselných i přirozených čtverců, dále na výsledky měření s ním spjaté, a pro zájemce nastíníme s odkazem na literaturu myšlenku velmi efektivního stochastického algoritmu, který náš problém řeší.

6.1 Algoritmus s posouváním

Nejprve si předestřeme poněkud jednodušší myšlenku algoritmu, jenž je uveden v dodatku A. Algorimus pro zadané číslo N vrací nezáporná celá čísla x_1, x_2, x_3 taková, že $N = x_1^2 + x_2^2 + x_3^2$. Funkce má druhý, volitelný argument `bez_nul`. Jedná se o příznak, který při nastavené hodnotě 1 algoritmu uloží, aby hledal pouze nenulová x_1, x_2, x_3. Jednička je také hodnota tohoto příznaku, pakliže při volání funkce není explicitně řečeno jinak. Samotnou logiku našeho algoritmu můžeme shrnout v následujících bodech:

1. Nejprve je na základě Věty 3.7 ověřeno, zda je vůbec možno číslo N rozložit na součet tří druhých mocnin celých čísel. Jinými slovy, zadané N dělíme číslem 4, dokud je to možno beze zbytku. Poté se ptáme, zda je zůstatek kongruentní se $7 (\mathrm{mod}\ 8)$. Pokud ne, číslo lze rozložit.

2. Pokud je rozklad možný, vezmeme nevyšší možné x_1, tj. $\left\lfloor \sqrt{N} \right\rfloor$. Pak položíme $a_1 = N - x_1^2$ a toto číslo se dále pokoušíme rozložit na dva čtverce.

3. V tomto kroku máme poměrně zkomplikovanou situaci. Na základě Věty 3.4 bychom pro ověření, zda lze a_1 rozložit na součet dvou čtverců potřebovali znát jeho kanonický rozklad. Žádný efektivní algoritmus pro hledání kanonického rozkladu čísla však není znám, a tak se může stát, že náš algoritmus bude hledat něco, co není možno nalézt. Jako hrubé síto nám poslouží alespoň nutná podmínka (viz Věta 3.3).

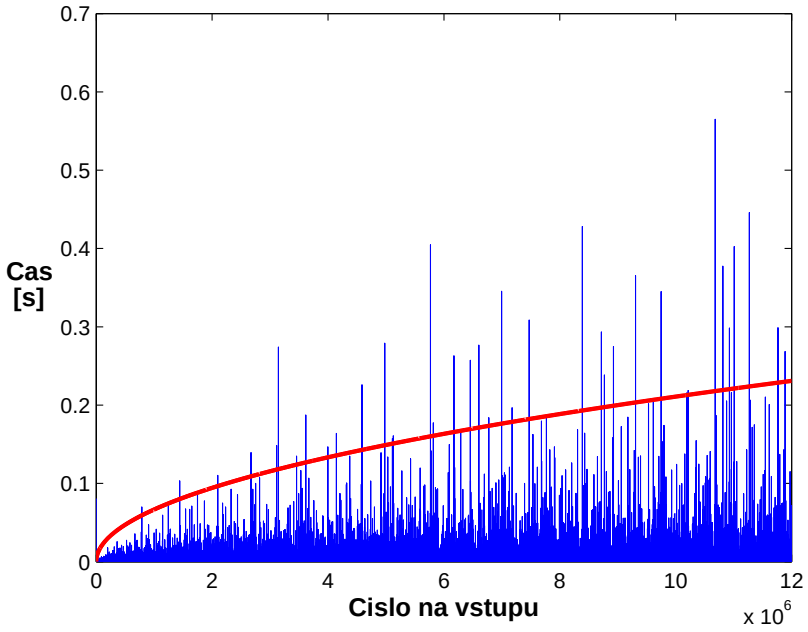
4. Dále postupujeme stejnou logikou jako dříve, x_2 zvolíme jako $x_2 = \lfloor \sqrt{a_1} \rfloor$, položíme $a_2 = a_1 - x_2^2$ a zjišťujeme, zda je samo a_2 čtvercem. Pokud ano, pak $x_3 = \sqrt{a_2}$ a algoritmus končí. V případě, že ne, zmenšujeme x_2 o jedničku, dokud nenalezneme dvoučtvercový rozklad nebo dokud má snižování x_2 smysl.

5. V případě, že a_1 nebylo možno rozložit na dva čtverce, vracíme se do 2. bodu a x_1 zmenšujeme o jedničku, opět dokud se nově vzniklé a_1 nepodaří rozložit na dva čtverce, eventuálně při požadavku na nenulovost, dokud to má smysl.

6. Pokud požadujeme nenulovost čísel x_1, x_2, x_3 a rozklad se nepodaří nalézt, algoritmus vrací $x_1 = x_2 = x_3 = -1$.

Úskalí tohoto algoritmu je zjevné. Může se stát, že proiterujeme spoustu možných a_1 neúspěšně. Navíc, když hledáme tříčtvercový rozklad bez nul u čísla, pro nějž jej není možno nalézt, algoritmus prozkoumá všechny možné varianty a pak bez úspěchu skončí.

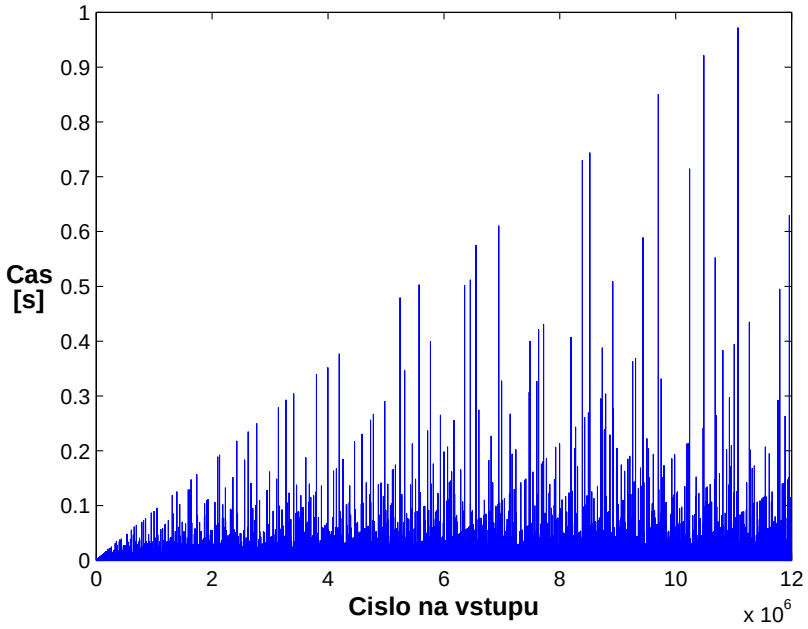
Reálná časová složitost však není tak problematická, jak by se mohlo zdát. Pro účel ilustrace časové náročnosti algoritmu bylo provedeno měření. Obrázek 5 ukazuje časovou náročnost výpočtu rozkladu (včetně nul) pro prvních deset milionů čísel z množiny B_3.



Obrázek 5: Časová náročnost algoritmu s posouváním, proložená křivkou $f(N) = \frac{\sqrt{N}}{15000}$

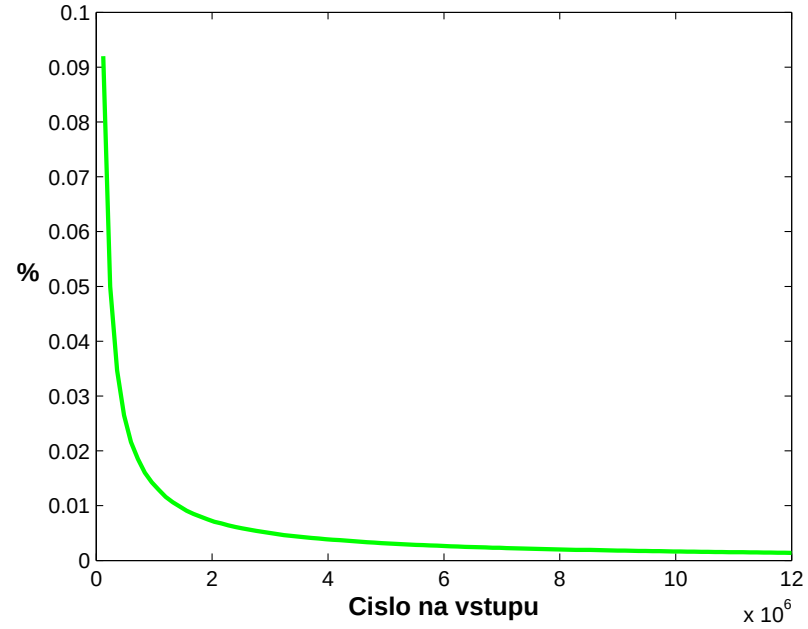
Algoritmus je zjevně lehce nestabilní, ale to nám vadit nemusí, jelikož vidíme, že u nejproblematičtějšího čísla rozklad trval přibližně 0,6 sekundy. Můžeme tak algoritmus označit za dostatečně účinný pro naše potřeby. Zajímavostí je jistě i skutečnost, že pouhých 39 z oněch deseti milonů měřených čísel mělo rozklad pomalejší, než $\frac{\sqrt{N}}{15000}$ sekund. Tento fakt by mohl být námětem ke studiu vlastností tříčtvercových čísel v kombinaci s teorií složitosti algoritmů v rámci teoretické informatiky.

Když se zaměříme na striktní požadavek na nenulovost čtverců, při kterém nám algoritmus řekne, zda je číslo prvkem množiny S_E, dozvíme se z měření vcelku očekávané výsledky. O něco častěji docházelo k časově náročnějším rozkladům blížícím se lineární složitosti, protože u části čísel, ač bylo možno rychle nalézt rozklad, musel algoritmus hledat dále, vzhledem k požadavku na nenulovost. V průměrném případě byl také algoritmus samozřejmě pomalejší, stejně tak nejnáročnější rozklad trval déle, nežli v případě bez nenulového požadavku.



Obrázek 6: Časová náročnost algoritmu s posouváním při ignorování nulových čtverců

Podle Věty 4.6 jde podíl čísel z množiny B_3, která nelze rozložit na tři nenulové čtverce s rostoucím N k nule. Jak vidíme na Obrázku 7, dokonce již pro relativně nízká čísla je jejich podíl poměrně zanedbatelný.



Obrázek 7: Relativní četnost výskytu čísel, striktně obsahujících nulové čtverce

6.2 Rabinův-Shallitův algoritmus

Závěrem krátce uveďme několik informací o efektivnějším algoritmu. V 80. letech se otázkou rozkladů čísel na součet celočíselných čtverců zabývali Michael O. Rabin a Jeffrey O. Shallit. Pomocí stochastických metod dospěli k výjimečně efektivním procedurám. V určitých případech však nečerpali jen z ryzí matematiky a logiky, nýbrž také z měření a z předpokládáné platnosti Riemannovy hypotézy. Ve stručnosti nastiňme nejzákladnější myšlenku jednoho z algoritmů, který bychom mohli využít k hledání rozkladu čísla na součet tří celočíselných čtverců. Zájemce o další algoritmy a podrobnější rozpravu, především pak o důkaz korektnosti, odkážeme na samotný článek obou výše zmíněných pánů [13].

Alternativní možností rozkladu na součet tří čtverců je hledat rozklad čísla na součet čtyř čtverců, a pro naše účely pak vybrat rozklad, jenž obsahuje právě jeden nulový čtverec. Rozklad na čtyři čtverce je ve článku [13] realizován pomocí **kvaternionové algebry**.

Definice 6.1 *Množinou **kvaternionů** nazveme množinu všech čísel ve tvaru* $a + bi + cj + dk$, *kde* $a, b, c, d \in \mathbb{R}$, $i^2 = j^2 = k^2 = ijk = -1$ *a*

$$\begin{aligned} ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j. \end{aligned}$$

Poznámka 6.1 Dodejme, že množinu všech kvaternionů označujeme $\mathbb{H}$. Jak vidíme z definice, kvaterniony jsou jakési zobecnění komplexních čísel, které je však nekomutativní na násobení. Stejně jako u komplexních čísel zavádíme ke kvaternionu $h = a + bi + cj + dk$ pojem sdruženého kvaternionu ve tvaru $\overline{h} = a - bi - cj - dk$, přičemž platí $h \cdot \overline{h} = \overline{h} \cdot h = a^2 + b^2 + c^2 + d^2$ a $\|h\| = \sqrt{h\overline{h}} = \sqrt{\overline{h}h}$.

Uvážíme-li $\mathbb{H}(\mathbb{Q})$ jako množinu všech kvaternionů, jejichž koeficienty a, b, c, d jsou racionální, lze ukázat, že ke každému kvaternionu $h_q \in \mathbb{H}(\mathbb{Q})$ existuje „blízký“ kvaternion $h_2 \in \mathbb{H}\left(\frac{1}{2}\right)$ (tedy kvaternion, jehož koeficienty jsou pouze násobky jedné poloviny) takový, že $\|h_q - h_2\| \leq \frac{1}{2}$. S jeho pomocí pak můžeme za užití Euklidova algoritmu nalézt **největší společný dělitel zprava** dvou kvaternionů, značíme $\gcd(h_1, h_2)$. Tento je analogií klasického největšího společného dělitele na nekomutativním násobení kvaternionů.

Uvedených faktů lze užít pro rozklad čísla N na čtyři čtverce. Základní myšlenkou algoritmu je pravděpodobnostní nalezení čísel $a, b \in \mathbb{Z}$ takových, že $a^2 + b^2 \equiv -1 (\mathrm{mod}\ N)$. Poté spočítáme $\gcd(a + bi + j, N)$. Výsledkem by měl být kvaternion, pro jehož koeficienty a, b, c, d platí

$$\begin{gathered} (a, b, c, d) = \chi \cdot (u, v, w, z),\ N = u^2 + v^2 + w^2 + z^2, \\ \chi \in \left\{ m \cdot \varepsilon | m \in \mathbb{Z}, \varepsilon \in \mathbb{H}\left(\frac{1}{2}\right), \|\varepsilon\| = 1 \right\}. \end{gathered}$$

7 Závěr

Zrekapitulujeme-li si naše počínání, seznámili jsme se s kvantovou mechanikou, vyřešili jsme problém částice v nekonečně hluboké pravoúhlé potenciálové jámě, podívali se na spektrum energií částice z hlediska teorie čísel, zkonstruovali jsme myšlenkový experiment s měřením energií v jámě a nalezli odhad počtu částic v ní, a nakonec sestrojili algoritmus, který by nám pomohl určit, zda naměřené energie spadají do energetického spektra částice.

Jak již ale bylo nastíněno úvodem, rovina, v níž jsme se pohybovali, byla poměrně dosti teoretická, zvídavého čtenáře tedy mohou napadnout přirozené otázky typu: „Fungovalo by to v praxi? Do jaké míry předestřené úvahy korespondují s reálnou situací?“, a mnoho dalších.

Pokud se například podíváme na náš myšlenkový experiment s měřením energií ryze fyzikálním způsobem, musíme především uvážit, že pokud by se v jámě nacházely elektrony (nebo obecně jakékoliv fermiony), pak by žádné dvě částice nemohly mít stejný kvantový stav. Další věcí je, že při změnách energie v jámě by bylo na místě pro možné kvantové stavy částic při měření uvážit tzv. Fermiho-Diracovo rozdělení (viz [3]), popisující jaké energetické hladiny okupují částice v systému složeném z fermionů za určité teploty. Přípustných námitek z pohledu fyziky je samozřejmě možno nalézt více.

Nezbývá než připustit, že ač by se naše úvahy za určitých okolností mohly lehce přiblížit reálné situaci, stále se v této práci jedná o jakousi myšlenkovou hru, jejímž účelem bylo především seznámit čtenáře se zajímavými souvislostmi mezi užitými disciplínami, zamyslet se nad stanovenými problémy a ilustrovat vybrané poznatky z teorie čísel, statistiky a fyziky.

Literatura

[1] Beiser A.: *Perspectives of Modern Physics*, New-York: McGraw-Hill, 1969.

[2] Skála L.: *Úvod do kvantové mechaniky*, Praha: Karolinum, 2011.

[3] Kvasnica J.: *Statistická fyzika*, Praha: Academia, 1998.

[4] Kolibiar M., Legéň A., Šálát T., Znám Š.: *Algebra a príbuzné disciplíny*, Bratislava: Alfa, 1992.

[5] Anděl J.: *Základy matematické statistiky*, Praha: Matfyzpress, 2007.

[6] Jahoda P.: *Vyjádřitelnost přirozených čísel v některých speciálních tvarech a množiny nulových asymptotických hustot*, disertační práce, Ostravká univerzita, 2005.

[7] Jahoda P.: *Notes on the expression of natural numbers as sum of powers*, Tatra Mt. Math. Publ. 34, str. 1-11, 2005.

[8] Krajc B., Beremlijski P.: *Obyčejné diferenciální rovnice*, PDF dostupné online na `http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/obycejne_diferencialni_rovnice.pdf`.

[9] Drábek P., Holubová G.: *Parciální diferenciální rovnice*, skripta ZČU Plzeň, 2001.

[10] Kufner A.: *Geometrie Hilbertova prostoru*, Praha: SNTL - Nakladatelství technické literatury, 1975.

[11] Kracík J.: *Poznámky k předmětu Statistika 3*, PDF dostupné online na `http://homel.vsb.cz/~kra0220/sta3/sta3.pdf` .

[12] Heaslet M.A., Uspensky J.V.: *Elementary number theory*, New-York: McGraw-Hill, 1939.

[13] Rabin M.O., Shallit J.O.: *Randomized algorithms in number theory*, Communications on Pure and Applied Mathematics, 39/S1, str. 239-256, 1986.

[14] Robert C.P.: *The Bayesian choice: from decision-theoretic foundations to computational implementation*, New York: Springer Science & Business Media, 2007.

A Algoritmus rozkladu čísel na součet tří čtverců

K práci přikládáme algoritmus s posouváním, uvedený v Kapitole 6, včetně ukázky několika jeho výstupů. Kód algoritmu lze také nalézt na přiloženém CD, společně s následujícími skripty, užitými při měření:

- Skript `cisla_test.m`, jenž generuje prvních deset milionů čísel, která je možné rozložit na součet tří čtverců celých čísel, a následně je ukládá do vektoru `cisla`.
- Funkce `mereni_rozkladu.m` má jako vstupní parametry vektor čísel a příznak `bez_nul`. Její úlohou je spočítat dobu, potřebnou k rozkladu čísel, obsažených ve vstupním vektoru, na součet tří čtverců. Výstupem funkce jsou výsledky měření a graf závislosti času rozkladu na rozkládaném čísle.
- Funkce `mereni_cetnosti.m` přijímá vektor čísel, tato čísla pak bere jako n, k nimž určuje $\frac{(B_3-S_E)(n)}{n}$ v procentech. Výstupem je opět, krom vlastních naměřených hodnot, také graf.

Závěrem poznamenejme, že implementace i měření byly provedeny v softwaru Matlab R2014a.

```
1  function xx = legendre(N, bez_nul)
2      if nargin == 1
3          bez_nul = 1;
4      end
5      N2 = N;
6      xx = -1*ones(1,3);
7      q = zeros(1,2);
8      a = zeros(1,2);
9      while mod(N2,4) == 0 && N2 ~= 0
10         N2 = N2/4;
11     end
12     if mod(N2,8) == 7
13         error('Zadane cislo nelze  rozlozit  na soucet 3 ctvercu.')
14     else
15         while 1
16             xx(1) = floor(sqrt(N)) - q(1);
17             a(1) = N - xx(1)^2;
18             if mod(a(1),4) == 3
19                 q(1) = q(1) + 1;
20                 continue;
21             elseif a(1) > 2*N/3
22                 xx = -1*ones(1,3);
23                 break;
24             else
25                 q(2) = 0;
26                 while 1
27                     xx(2) = floor(sqrt(a(1))) - q(2);
```

```
                    a(2) = a(1) - xx(2)^2;
                    if a(2) > a(1)/2
                        break;
                    elseif mod(sqrt(a(2)),1) == 0
                        xx(3) = sqrt(a(2));
                        break;
                    else
                        q(2) = q(2) + 1;
                        continue;
                    end
                end
                if xx(3) == -1
                    q(1) = q(1) + 1;
                    continue;
                elseif bez_nul
                    if sum(xx==0)>0
                        q(1) = q(1) + 1;
                        continue;
                    else
                        break;
                    end
                else
                    break;
                end
            end
        end
    end
end
```

Výpis 1: Algoritmus rozkladu čísla na 3 čtverce s posouváním v jazyce Matlab

```
>> legendre(23)
Error using legendre (line 15)
Zadane cislo nelze rozlozit na soucet 3 ctvercu.

>> legendre(29)

ans =
4     3     2

>> legendre(29, 0)

ans =
5     2     0

```

```
>> legendre(37,0)

ans =
6     1     0

>> legendre(37)

ans =
-1    -1    -1

>> tic; legendre(123456789123456789), toc;

ans =
351364178      58440      11252

Elapsed time is 0.127374 seconds.

>> tic; legendre2(666^2+66^2+6^2), toc;

ans =
666    66     6

Elapsed time is 0.001367 seconds.
```

Výpis 2: Ukázky výstupů algoritmu s posouváním